REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*

2. REPORT DATE
7 June 1996

3. REPORT TYPE AND DATES COVERED
Master's Thesis, 2 Aug 95-7 June 1996

4. TITLE AND SUBTITLE
AN OBJECTIVE INFORMATION ARCHITECTURE FOR THE ARMY OF THE TWENTY- FIRST CENTURY: COURTING ATHENA

5. FUNDING NUMBERS

6. AUTHOR(S)
MAJ Richard E. Volz, Jr., U.S. Army

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
U.S. Army Command and General Staff College
ATTN: ATZL-SWD-GD
Fort Leavenworth, Kansas 66027-1352

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited

DTIC QUALITY INSPECTED 4

12b. DISTRIBUTION CODE
A

13. ABSTRACT *(Maximum 200 words)*
This study investigates the current division level Command, Control, Communications, Computers and Intelligence (C4I) information architecture and its ability to support Army divisions in the twenty-first century. Current developmental efforts are examined to determine their ability to support the warfighting Commander's Critical Information Requirements. The study then explores trends in information technology under development within commercial industry. A conceptual information architecture, Athena, is then presented to meet warfighting requirements while maximizing limited tactical communication resources. Information technologies are being developed to support a wide variety of battlefield functions. Current developmental efforts are diffuse and costly. A single information system architecture is needed if the Army is employ information technologies as a combat multiplier. The Athena Information Architecture employs distributed, object-oriented database technology to achieve true interoperability of information. Athena is a single information system for all Battlefield Functional Areas. It brings together warfighting requirements and emerging commercial technologies within the constraints of a highly mobile and lethal Army force. The Athena architecture is focused on a single goal; enabling the warfighting commander to achieve information dominance to defeat America's enemy and minimize the loss of United States soldiers.

14. SUBJECT TERMS
Athena, Information Architecture, Distributed Databases, Software Agents, Network, Force XXI

15. NUMBER OF PAGES
88

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED

GENERAL INSTRUCTIONS FOR COMPLETING SF 298

The Report Documentation Page (RDP) is used in announcing and cataloging reports. It is important that this information be consistent with the rest of the report, particularly the cover and title page. Instructions for filling in each block of the form follow. It is important to ***stay within the lines*** to meet ***optical scanning requirements***.

Block 1. Agency Use Only *(Leave blank)*.

Block 2. Report Date. Full publication date including day, month, and year, if available (e.g. 1 Jan 88). Must cite at least the year.

Block 3. Type of Report and Dates Covered. State whether report is interim, final, etc. If applicable, enter inclusive report dates (e.g. 10 Jun 87 - 30 Jun 88).

Block 4. Title and Subtitle. A title is taken from the part of the report that provides the most meaningful and complete information. When a report is prepared in more than one volume, repeat the primary title, add volume number, and include subtitle for the specific volume. On classified documents enter the title classification in parentheses.

Block 5. Funding Numbers. To include contract and grant numbers; may include program element number(s), project number(s), task number(s), and work unit number(s). Use the following labels:

C	- Contract	**PR**	- Project
G	- Grant	**TA**	- Task
PE	- Program Element	**WU**	- Work Unit Accession No.

Block 6. Author(s). Name(s) of person(s) responsible for writing the report, performing the research, or credited with the content of the report. If editor or compiler, this should follow the name(s).

Block 7. Performing Organization Name(s) and Address(es). Self-explanatory.

Block 8. Performing Organization Report Number. Enter the unique alphanumeric report number(s) assigned by the organization performing the report.

Block 9. Sponsoring/Monitoring Agency Name(s) and Address(es). Self-explanatory.

Block 10. Sponsoring/Monitoring Agency Report Number. *(If known)*

Block 11. Supplementary Notes. Enter information not included elsewhere such as: Prepared in cooperation with...; Trans. of...; To be published in.... When a report is revised, include a statement whether the new report supersedes or supplements the older report.

Block 12a. Distribution/Availability Statement. Denotes public availability or limitations. Cite any availability to the public. Enter additional limitations or special markings in all capitals (e.g. NOFORN, REL, ITAR).

- **DOD** - See DoDD 5230.24, "Distribution Statements on Technical Documents."
- **DOE** - See authorities.
- **NASA** - See Handbook NHB 2200.2.
- **NTIS** - Leave blank.

Block 12b. Distribution Code.

- **DOD** - Leave blank.
- **DOE** - Enter DOE distribution categories from the Standard Distribution for Unclassified Scientific and Technical Reports.
- **NASA** - Leave blank.
- **NTIS** - Leave blank.

Block 13. Abstract. Include a brief *(Maximum 200 words)* factual summary of the most significant information contained in the report.

Block 14. Subject Terms. Keywords or phrases identifying major subjects in the report.

Block 15. Number of Pages. Enter the total number of pages.

Block 16. Price Code. Enter appropriate price code *(NTIS only)*.

Blocks 17. - 19. Security Classifications. Self-explanatory. Enter U.S. Security Classification in accordance with U.S. Security Regulations (i.e., UNCLASSIFIED). If form contains classified information, stamp classification on the top and bottom of the page.

Block 20. Limitation of Abstract. This block must be completed to assign a limitation to the abstract. Enter either UL (unlimited) or SAR (same as report). An entry in this block is necessary if the abstract is to be limited. If blank, the abstract is assumed to be unlimited.

AN OBJECTIVE INFORMATION ARCHITECTURE FOR THE ARMY OF THE TWENTY-FIRST CENTURY: COURTING ATHENA

A thesis presented to the Faculty of the U.S. Army Command and General Staff College in partial fulfillment of the requirements for the degree

MASTER OF MILITARY ART AND SCIENCE

by

RICHARD E. VOLZ, JR., MAJ, USA
B.S., Siena College, Loudonville, New York, 1983
M.S., Naval Postgraduate School, Monterey, California, 1991

Fort Leavenworth, Kansas
1996

AN OBJECTIVE INFORMATION ARCHITECTURE FOR THE ARMY OF THE TWENTY-FIRST CENTURY: COURTING ATHENA

A thesis presented to the Faculty of the U.S. Army
Command and General Staff College in partial
fulfillment of the requirements for the
degree

MASTER OF MILITARY ART AND SCIENCE

by

RICHARD E. VOLZ, JR., MAJ, USA
B.S., Siena College, Loudonville, New York, 1983
M.S., Naval Postgraduate School, Monterey, California, 1991

Fort Leavenworth, Kansas
1996

MASTER OF MILITARY ART AND SCIENCE

THESIS APPROVAL PAGE

Name of Candidate: MAJ Richard E. Volz, Jr.

Thesis Title: An Objective Information Architecture for the Army of the Twenty-First Century: Courting Athena

Approved by:

____________________________, Thesis Committee Chairman
MAJ Howard R. Cuozzi, M.F.A.

____________________________, Member
MAJ Deborah A. Valentine, B.S.

____________________________, Member
SFC John T. Broom, Ph.D.

Accepted this 7th day of June 1996 by:

____________________________, Director, Graduate Degree Programs
Philip J. Brookes, Ph.D.

The opinions and conclusions expressed herein are those of the student author and do not necessarily represent the views of the U.S. Army Command and General Staff College or any other governmental agency. (References to this study should include this statement.)

ABSTRACT

AN OBJECTIVE INFORMATION ARCHITECTURE FOR THE ARMY OF THE TWENTY-FIRST CENTURY: COURTING ATHENA by MAJ Richard E. Volz, Jr., USA, 88 pages.

This study investigates the current division level Command, Control, Communications, Computers and Intelligence (C4I) information architecture and its ability to support Army divisions in the twenty-first century. Current developmental efforts are examined to determine their ability to support the warfighting Commander's Critical Information Requirements. The study then explores the trends in information technology under development within commercial industry. A conceptual information architecture, Athena, is then presented to meet warfigting requirements while maximizing limited tactical communication resources.

Information technologies are being developed to support a wide variety of battlefield functions. Current developmental efforts are diffuse and costly. A single information system architecture is needed if the Army is to employ information technologies as a combat multiplier.

The Athena Information Architecture employs distributed, object-oriented database technology to achieve true interoperability of information. Athena is a single information system for all Battlefield Functional Areas. It brings together warfighting requirements and emerging commercial technologies within the constraints of a highly mobile and lethal Army force. The Athena architecture is focused on a single goal; enabling the warfighting commander to achieve information dominance to defeat America's enemy and minimize the loss of United States soldiers.

ACKNOWLEDGEMENTS

There are many people I wish to thank for their assistance with this thesis and the developmental of the Athena architecture. Athena was conceived in the newly established Architecture Branch, Directorate of Combat Developments, Fort Gordon, GA. It represents the efforts and ideas of the finest group of individuals, both military and civilian, with whom I was privledged to serve from 1991 through 1995. Greatly overworked, this ensemble of professional individuals, continue to develop and deliver the finest military communications equipment in the world. While there is insufficient space here to name them all, I would like to recognize a few individuals without whose help I would have been unable to complete this work.

My thanks to CW3 Dan DeWaal for allowing me to bounce my ideas off him during many late nights at Signal Towers. SFC Tony Loop, a great NCO and a good friend, who injected reality into Athena and helped me keep the architecture within the limits of the possible. To MAJ Tony Blando, a great friend and peer, who's enthusiasm always kept me going whenever I became bogged down in the process of writing. To MG Douglas D. Buchholz, who always gave me the freedom to explore new solutions for the Army's communication problems and provided his full support in all my efforts. Words of thanks are not enough to express my graditude to COL Robert L. Forrester for his guidance, mentorship and support through the entire development of the Athena Architecture. The day COL Forrester retires from active duty will be a major loss to the Signal Corps and the Army at large. He is one of the most dedicated and knowledgable leaders I have had the privledge to know.

My experiences at Command and General Staff College were invaluable in the creation of Athena. Of particular support were all the members of Staff Group 2C and our leader LTC White. Three good friends, MAJs Chuck Hardy, Val Ruffo, and Sandy Young provided the warfighter perspective necessary to make Athena a viable solution. To MAJ Jim Davidson, my Tactics instructor, who provided a great deal of his free time to ensure that even a signal officer, such as myself, could understand maneuver warfare. His insights as a member of the Opposing Force at the National Training Center helped ensure Athena met the needs of the warfighting commander. To my entire Thesis Committee, for their patient support and invaluable advice.

Finally, and most especially, to my daughter, Rachel. Although she lives many miles away, she is always in my heart and thoughts. The Athena architecture is dedicated to her, her future and the future of all America's children. The Athena architecture means winning the information war and defeating America's enemies without firing a single shot in anger.

TABLE OF CONTENTS

LIST OF ILLUSTRATIONS

LIST OF ABBREVIATIONS

ABCS	Army Battle Command Systems
AFATDS	Advanced Field Artillery Target Designation System
ANM	Automated Network Manager
AO	Area of Operations
ASAS	All Source Analysis System
ATA	Army Technical Architecture
ATCCS	Army Tactical Command and Control System
AT&T	American Telephone and Telegraph
AWE	Advanced Warfighting Experiment
BDE	Brigade
BOS	Battlefield Operating System
CCIR	Commander's Critical Information Requirements
CCP	Contingency Communication Package
CECOM	Communication Electronics Command
CHS	Common Hardware Software
CIA	Central Intelligence Agency
COE	Common Operating Environment
COTS	Commercial Off The Shelf
CSSCS	Combat Service Support Control System
C2	Command and Control
C3	Command, Control and Communications

C4I	Command, Control, Communications, Computers, and Intelligence
C4IEW	Command, Control, Communications, Computers, Intelligence, and Electronic Warfare
DIS	Defense Information System
DISCOM	Division Support Command
DISC4	Directorate of Information Systems for Command, Control, Communications and Computers
DoD	Department of Defense
DOM	Distributed Object Manager
DTAC	Division Tactical Command Post
DTOC	Division Tactical Operation Center
EPLRS	Enhanced Position Location Reporting System
FAADC2I	Forward Area Air Defense Command, Control, and Intelligence
FM	Field Manual
FSB	Forward Support Battalion
FSC3	Fire Support Command, Control, and Coordination
GUT	Generic User Terminal
HQ	Headquarters
IEW	Intelligence and Electronic Warfare
IMC	Information Management Center
JSTARS	Joint Surveillance Target Attack Radar System
kbps	kilobits per second
LAN	Local Area Network
LBE	Load Bearing Equipment
LEN	Large Extention Node

LIN	Large Information Node
mbps	megabits per second
MCS	Maneuver Control System
MCS/P	Maneuver Control System/Pheonix
MIN	Medium Information Node
MOS	Military Occupation Specialty
MSE	Mobile Subscriber Equipment
MSF	Mobile Strike Force
NCO	Non Commissioned Officer
NCS	Node Center Switch
ORD	Operational Requirements Document
PIR	Priority Information Requirements
R&D	Research and Development
SEN	Small Extension Node
SIDPERS	Single Integrated Personnel System
SIN	Small Information Node
SINCGARS	Single Channel Ground Airborne Radio System
SIV	System Integration Van
TI	Tactical Internet
TOC	Tactical Operation Center
VTC	Video Teleconferencing

CHAPTER 1

INTRODUCTION

Purpose

The Army, as well as its sister services, has recognized that interoperability is a major concern. This thesis will examine interoperability among the battlefield operating systems within the Army as it pertains to information technology. It will evaluate existing Command and Control (C2) systems and their relationship to battle command in order to propose an optimal information architecture. An optimal information architecture is one that allows the warfighting commander and his staff to focus on battle command, not information gathering and processing. This architecture can act as the blueprint for the development of future information systems whether they support the C2 process or individual weapons platforms.

Research Question. The fundamental question to be answered is; what is the optimal C2 information architecture for the Army in the twenty-first century that will magnify the effectiveness of battle command.

Secondary research questions that support an optimal C2 information architecture are as follows:

1. Why should the Army change its current information architecture strategy?

2. How are the commander's critical information requirements met?

3. How is data most effectively passed over tactical communications?

4. What information network services will be required?

5. What technologies are available to support an information architecture?

6. How should the Army organizationally support an information architecture?

7. How does the Army redefine signal support?

Scope

This effort will focus on information systems at Division and below; however, the principles may be applied throughout the Joint community. It will explore the systems that will be fielded over the next ten years and examine the implications of current functional area unique approaches; often referred to as "stovepipe" systems due to their lack of interoperability with other information systems. Technologies under development within commercial industry will also be examined so that an architecture can be developed that will compliment commercial endeavors, ensuring that the Army will continue to be able to leverage commercial technology.

Importance

An investigation into this area is recommended if the Army are to best meet the commander's information requirements within physical limitations and current budgetary constraints. The warfighting commander's need for increased information, along with greater increases in mobility and lethality, drive the need for this evaluation. Communications on the modern battlefield are limited by the need for mobility. The greater the need for information within the tactical headquarters, the greater the reduction of that headquarters' mobility. C2 systems must be developed in a manner which enhances the commander's ability to command and control his forces while maintaining their mobility and survivability.

Problem Statement

Command and Control (C2) systems are being developed with a bottom-up approach. While this appears to meet the needs of the warfighter on the surface, there are numerous far-reaching implications of such a developmental process. The current bottom-up approach does not examine the questions of network capacity, interoperability, network services, and associated costs. Costs include dollars, manpower, and limited functionality.

Cost in Dollars. Large portions of the C2 system budgets are being wasted on redundant capabilities among each Army proponent's system. Each C2 system is independently developing databases that have many overlapping data elements. These data elements and message formats need to conform to a common set if interoperability is to be achieved and waste is to be reduced. The same is true for processing algorithms. How C2 systems process information requests and actions should be standard across the Army, not uniquely developed for each system. Reuse of previously developed software reduces Army costs across all information systems.

Cost in Manpower. In addition to the increased burden these information requirements place on battlefield communications, there is another challenge to which the user community is only now becoming aware. The fielding of multiple information systems on the battlefield and the challenges of incorporating these systems into a unified command and control system create the need for information management and services. The vast majority of Army units employ specially trained personnel to employ and manage their networks while in garrison. This information network infrastructure allows users to focus on their primary mission, whether it be command of an infantry company or running a large depot. The Army community cannot expect users to install, operate, and maintain large networks and remain focused on their primary responsibilities. An investment in the battlefield infrastructure must be made if the Army is to reap the benefits of battlefield automation.

A bottom-up approach precludes the inclusion of an infrastructure to support user applications. The lack of a standard infrastructure results in user terminals which are highly complex and not user friendly. This complexity drives the need for additional soldiers to install, operate, and maintain C2 systems than were originally proposed as a manpower savings.

Cost in Functionality. Current C2 system solutions, developed in isolation, do not consider the impact of other systems on their applications. Government contractors developing inefficient processing techniques fail to recognize the existence of other systems which must all share the same bandwidth. As these systems are fielded to the force structure, commanders will come to the realization that all battlefield applications will not fit within their communication resources. Commanders will be forced to decide which automated functionality can be provided on the battlefield and which cannot. If the function of situational awareness is the commanders' highest priority, he may be forced to eliminate automated logistical support from his C2 architecture. This is a major example of poor system engineering.

Current commercial industry efforts are based on high capacity, fixed station infrastructures. Information exchanges take place over multiple T-1 (1.544 megabits per second (mbps)) digital trunk groups in support of a myriad of commercial enterprises. Communication pipelines on the battlefield range from 1152 kilobits per second (kbps) at Echelons Above Corps (EAC) to 9.6 kbps within the maneuver brigade. Increases in this capacity are forthcoming, but will in no way match the rate at which the warfighter's information requirements continue to grow. The Army cannot afford a wholesale replacement of its communications network. The price can only be paid in a loss of functionality.

Cost in System Complexity and User Burden. The lack of a supporting infrastructure within any information architecture results in highly complex user terminals. User terminals of greater complexity place increased burdens on the warfighter. Each warfighter will require extensive training in order to be able to operate a user device. The responsibility for information services, normally provided by a network infrastructure, falls squarely on the shoulders of the warfighter.

These additional functions will distract the user from accomplishing critical mission tasks. The goal of any information system should be to allow the warfighter to focus on the business of fighting and winning America's wars, not sorting through databases and registering users.

Summary

This document will examine the problems inherent in currently funded Army information systems. It will define principles of information and communication network design and apply them against current efforts. Finally, those previously defined principles will be used to design an information architecture from the top-down which meets the warfighter's requirements from the bottom-up. The proposed information architecture must meet the warfighting requirements of today and provide ample room for growth into the future.

CHAPTER 2

REVIEW OF CURRENT EFFORTS AND LITERATURE

Current Guidance

Advances in information technologies are occuring on a daily basis. The majority of technical information available on this subject is not found in traditional sources. Therefore, the principles and concepts described herein were developed through corporate and research documentation available on the World Wide Web. References to specific web sites are given where appropriate.

The Command, Control, Communications, Computers and Intelligence (C4I) for the Warrior concept, as presented by the Joint Chiefs of Staff, provides a unifying concept that will support warfighting needs and will meet the requirements of national security plans. The goal of the C4I for the Warrior concept is to provide the warfighting commander access to all the information required to win on the battlefields of the future. This information is to be presented when, where, and how the commander requires it. The concept provides a roadmap to achieve a worldwide information network that is secure, seamless, and timely.[1]

Army C4I Architecture

The C4I for the Warrior concept is an attempt to achieve interoperability among the various information systems throughout the Department of Defense. This challenge is mirrored within the Army's information systems. The Army's C4I architecture contains a myriad of information systems at all echelons and security levels. These information systems must be designed to support interoperation in order to achieve the maximum effect in supporting the warfighting commanders.

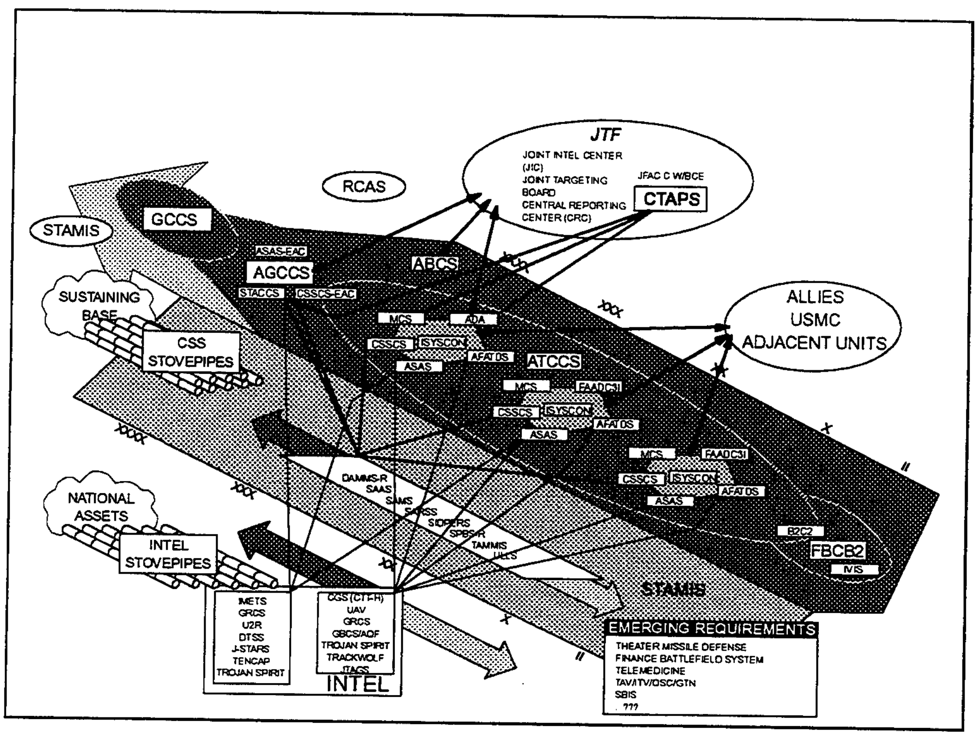

Figure 1. The Army's C4I Architecture.

The Army Enterprise Strategy, published by the Directorate of Information Systems for Command, Control, Communications, and Computers (DISC4) for the Chief of Staff of the Army, establishes a set of guidelines for the development of Army systems. The strategy describes principles and designates responsibilities necessary to insure battlefield interoperability. Figure 1 represents the Army's current C4I architecture. It also represents the challenges the Army must overcome if it is to be able to gain the full benefit of information technologies.[2]

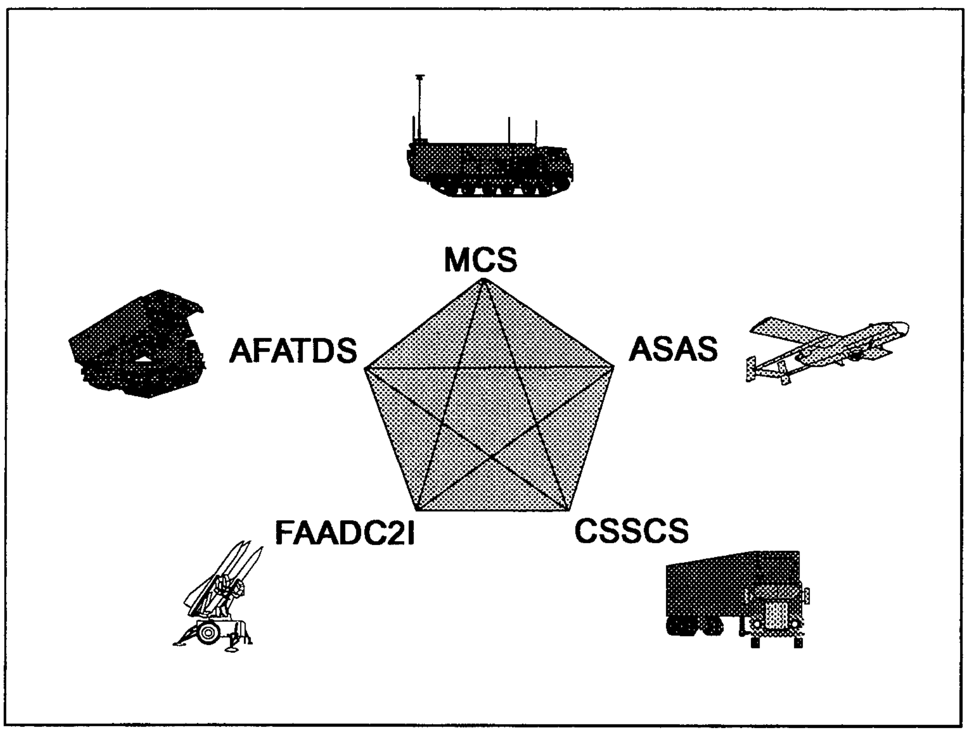

Figure 2. The Army Tactical Command and Control System.

Background

The Army's current effort at automating C2 for the warfighter is a myriad of diverse information systems developed by each of the Army's proponents. The central component of this architecture is the Army Tactical Command and Control System (ATCCS). An initial discussion of the ATCCS architecture is necessary to explore how the system developed and the limits it will place on the Force XXI Warfighter. A key work that decribes currently funded programs is the Command, Control, Communications, Computers, Intelligence and Electronic Warfare (C4IEW) Project Book distributed by the U.S. Army Communications Electronic Command (CECOM). The project book describes each command and control system that is currently funded. Each system's capabilities are described, as well as current program status and fielding schedules. Figure 2 depicts the ATCCS architecture and the communications connectivity required. The ATCCS consists of five subsystems as follows:

Maneuver Control System (MCS). MCS is a tactical computer network to automate the command and control process. Field commanders are provided the ability to receive, process, and transmit information and directives within the enemy's decision cycle. MCS computers will be found from battalion to Corps level.[3]

Advanced Field Artillery Tactical Data System (AFATDS). The goal of AFATDS is to automate the US Army Fire Support Command, Control, and Coordination (FSC3) system. AFATDS provides automated fire support within the ATCCS architecture in support of close, deep, and rear operations and to support the commander's scheme of maneuver.[4]

All Source Analysis System (ASAS). ASAS is the Intelligence and Electronic Warfare (IEW) subsystem of ATCCS. It will provide the intelligence community a tool to fuse all source intelligence to gain a timely view of the enemy's capabilities, deployments, and potential courses of action. Warfighting commanders will be able to see the battlefield more effectively and develop an appropriate scheme of maneuver.[5]

Forward Area Air Defense Command, Control, and Intelligence (FAADC2I) System. FAADC2I is an automation system that that provides the air defense community C2 and targeting information necessary to gain air superiority in a given theater of operations. The system will provide automated support to FAAD battalions and separate batteries.[6]

Combat Service Support Control System (CSSCS). CSSCS is an automation system designed to support the planning and execution of logistic operations. The system collects, processes, and disseminates CSS information in support of the commander's scheme of maneuver. The system links the functions of command and control and resource management.[7]

Joint Venture, the first leg of the Army's digitization strategy, focuses on the realignment of Army force structure based on information technology. It is an attempt to examine how information technologies will affect command and control processes and to determine the best organization of the commander's staff around automation. Joint Venture efforts are currently focused on the benefits of the ATCCS architecture. However, the ATCCS architecture, as defined above, represents the development of automation systems along traditional staff roles. The resulting reorganization will reflect the staff in its traditional manning. The nature of this architecture, by definition, precludes the development of a digitized staff.[8] Figure 3 depicts the resultant staff organization based on developing automation systems.

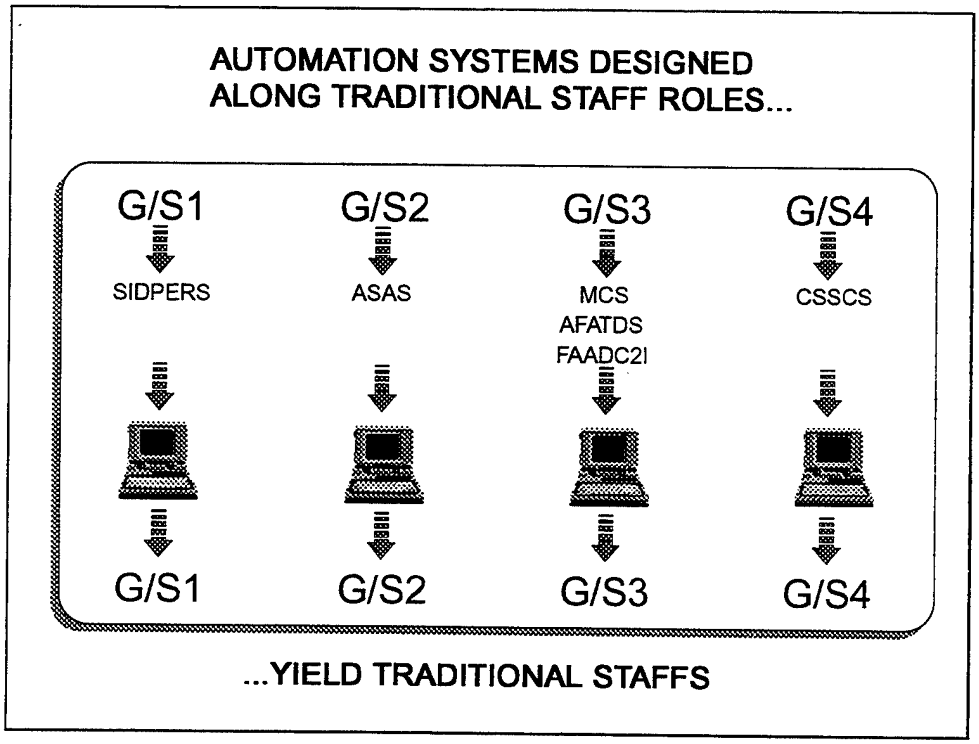

Figure 3. Stovepipe Staffs.

Information technologies should allow the commander to organize his staff based upon mission requirements. For example, the current battle staff organization may be appropriate for fighting a protracted conflict against a large, ground based force. However, during a humanitarian assistance operation the majority of the mission is focused on logistics support and force protection. The comander may desire to organize the battle staff to emphasis the nature and main effort of the operation. Current automation development strategies preclude the commander from doing so.

Information Technology

In order to properly explore this area, the Army must first examine why information systems exist as they are today. Limitations imposed by the physical world have constrained the way humans exchange and process information. The explosion of information technologies in the past two decades have removed the physical limitations of previous generations. However, most automation development efforts do not recognize the freedom afforded by information technologies. Most information systems merely automate a physical process. For example, battle staffs physically copy operational graphics onto acetate to facilitate planning. The product is called an overlay. Subordinate units then trace the overlay and transport it to their headquarters to facilitate planning among subordinate headquarters. ATCCS systems today use software to create overlays and then transmit those overlays to subordinate units via tactical communications. There are much more efficient ways to transmit the same information and tailor it to meet the needs of the warfighting commanders. It is of fundamental importance to the Army to break with the traditions of the past and reexamine the methods available to meet the commander's information requirements and determine how information technology can best support those needs.

Historical Limitations. Information exchange between commanders and their superiors and subordinates have been limited to means based upon the physical world. Information exchange requirements have been and continue to be defined along physical paths. Armies of the eighteenth century exchanged information by only two means, written or verbal messages. These messages could only be transmitted by foot, signal, or horse.

Information was provided to the commander in the form of reports. In the heat of battle, these reports were often verbal and could be easily misinterpreted by the commander, his staff, or the messenger. This information would then be evaluated by the commander and the appropriate response determined. Commanders then used similar means to send directives or requests for additional information. The commander was limited in his scheme of maneuver by the means available to deliver his intent.

The same is true today. Commanders are limited in their scheme of maneuver based on physical limitations. Their forces are organized based upon the commanders span of control. A force could be no larger than an individual commander could control. The addition of terrestrial and space based communications have done little to change this fact. Orders are still passed either verbally or orally regardless of the means employed.

Trends in Information Technology. The explosion of information and communication technologies create an unlimited range of possibilities for commanders, their staffs, and their soldiers. Information systems can provide the means to break the physical limitations of the past. A commander's span of control can increase greatly with the advantages provided by information systems. Units can be widely dispersed across the battlefield without the loss of control by the commander. Increased dispersal equals increased survivability of friendly forces.[9]

Commercial information industries have recognized that customers demand a system that is complex in the services it provides yet simple enough for the average person to use. This same principle applies on the modern battlefield. The complexity of information systems must be reduced so that the soldier does not become overwhelmed by the demands placed by those same systems. Battle staffs can quickly become absorbed in the business of updating and searching databases rather than focusing on the business of developing unique solution for unique missions. Industry is attempting to overcome this challenge.

Network Complexity. In order to support the demands of consumers, industries such as American Telephone and Telegraph (AT&T) are examining ways to provide information services. AT&T has recognized that providing information services to the general public is in many ways similar to providing communication services. An increase in the complexity of user services, demands devices that are smarter and therefore more complex. Increasing the complexity of the user's device increases the risk that the consumer will find the product too difficult to operate. Different models of the same device will operate differently.[10]

A method commonly used in the telecommunication industry to solve this problem is to make devices that are user friendly. This is done by placing the intelligence necessary to accomplish complex tasks within the network. Intelligent communication network services available today include call forwarding, voice mail, and conference calling. A unique device is not required to provide these services. The same should be true of information services.[11]

However, the Army must be careful not to wholeheartedly embrace all the trends of commercial industry. For the most part, current information technologies are based upon fixed land based infrastructures that provide large communication pipes (bandwidth). This infrastructure does not exist on the modern battlefield. Radio systems are the least favored of all communication means by industry because of inherent errors, bandwidth constraints, and decreased reliability. Army operations, on the other hand, demands a high degree of mobility. Mobility can only be achieved through the use of radio systems. In recognizing this self imposed limitation, we must develop an information system that exchanges information in the most efficient manner possible.

Preliminary investigation into this area by the Signal Center and the results of ATCCS III testing indicate that current communication systems cannot handle the data load and that there is no infrastructure to support the services warfighters require on the modern battlefield. Current solutions are focused on the near-term and are limited to specific systems. Communications are a limited resource on the battlefiled and must be used judiciously if the maximum effectiveness is to be achieved.[12]

Current information systems exchange entire databases in order to update a limited number of files. Position reports are transmitted both vertically and horizontally, at all echelons, to all users in order to generate a situational awareness picture. This is done regardless of the level of detail required. The information system must then filter out the unwanted information upon its arrival. This method requires that all position location reports are passed to all locations even if the information is never used. This approach is extremely inefficient and wastes the limited communication resources available. Figure 4 represents the balance that must be achieved between system software transmission efficiency and available communication resources.

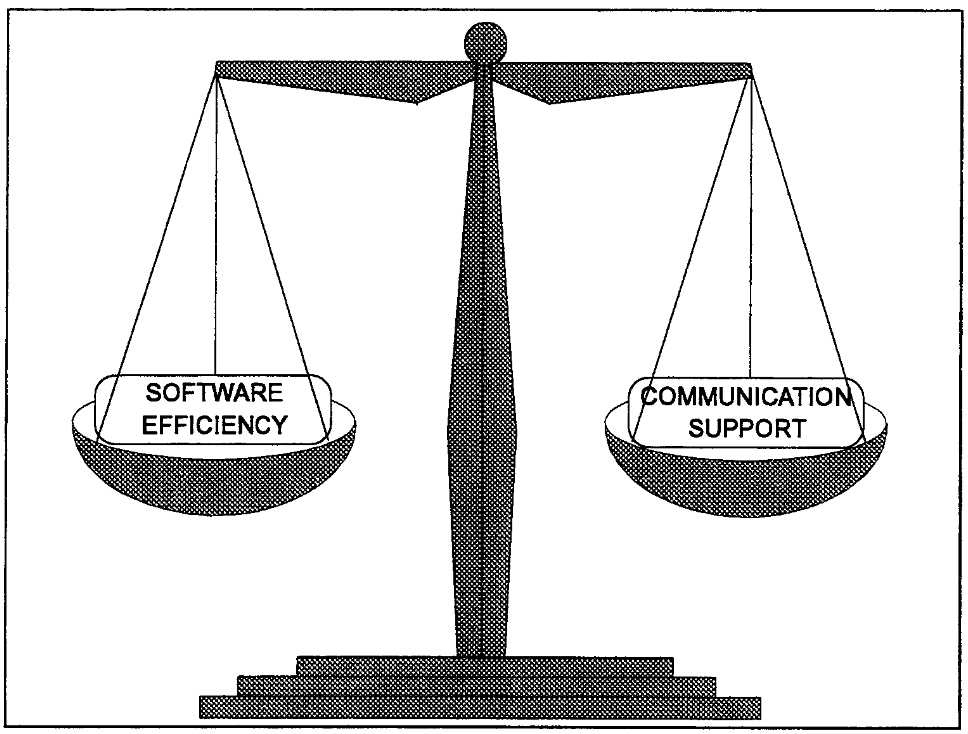

Figure 4. Information Transmission Efficiency versus Available Communications.

Self-Organizing Systems. Another way to limit the burdens automation can place on the commander and his staff is to develop software that can act independently. Direct manipulation of data will become a thing of the past as the demands made by users become more complex. Methods are being investigated to delegate these time consuming tasks to so-called "software agents." Software agents which know the requirements of the user, based on a preset user profile, act independently on the user's behalf. The process will become one of cooperation between the user and the information network. Self-organizing systems provide software agents that will search connected databases to find information that meets a users' needs.[13] For example, a commander may define a certain enemy unit as a high priority target and identify it as critical to the mission's success. Software agents will have the ability to traverse an entire information network and search for spot reports, sensor readings, and analyized imagery that meet the criteria defined by the commander. Once located the software agents report the correlated information to the commander. This is a task normally resigned to intelligence staffs and is extremely time consuming. Software agents can potentially relieve staffs of this burden and allow them to focus on analysis of enemy actions and prediction of future actions.

The use of artificial intelligence techniques will enhance a user' ability to manage information. The advent of the Internet exposes users to a vast mountain of information. Sorting through this wealth of information is a time consuming process and the mountain continues to grow in leaps and bounds. Users will require automated assistance that is both diligent and timely to solve complex problems. Artificial intelligence is a technology that will be demanded by the user community at large.[14]

Breaking the Physical Bounds. The introduction of these information technologies will tear down the physical limitations that constrain information exchange. Horizontal integration of multiple categories of information will become possible. The only limitation the Army will face will be self imposed. The Army must reevaluate the way it views command and control of forces and the staff process in light of technological advances.

Any advance in technology presents opportunities. However, technology can drive our requirements if we permit it. To procure a technology simply because it is available makes poor operational and fiscal sense. In the current environment of a shrinking budget, it is critical that we carefully evaluate the capabilities information technologies present and select those capabilities that meet warfighting requirements. From an informational standpoint, warfighting requirements can be defined as that information a commander must have if he is to successfully accomplish the mission. This informational solution set will vary based upon the given situation. The information required to perform peacekeeping operation will greatly differ from that required to conduct a ground offensive. However, all of the the information should be available within the area of operations. It then becomes a matter of accessing the appropriate information.

Command and Control. The warfighting commander must exercise effective command and control if the Army is to win on the battlefields of the twenty-first century. FM 100-5, Army Operations, provides the doctrinal foundation for any examination of C2 systems. It describes the way in which the warfighter intends to achieve victory on the battlefields of the early twenty-first century. FM 100-5 will be used extensively to examine each command, control, and communications (C3) systems' capability to support the needs of the warfighter. It will provide the doctrinal basis for an optimal information architecture.[15]

Commanders must be able to rapidly assimilate a vast amount of information and issue directives that are within a potential enemy's decision cycle. This enables commanders to impose their will on the enemy. Command, Control, and Communications Systems Engineering by Walter R. Beam provides an in-depth look into the various aspects of design, operation, and technologies particular to C3 systems. The principles and practices of management are also examined. Matters such as logistical support (provisions, utilities, repair, etc.), which are to be part of any information infrastructure are examined with regards to C3 design and use. Mr. Beam's descriptions were used as the starting point in this examination of Army information systems and the foundation for the design of an optimal information network.[16]

Common Picture of the Battlefield. Presenting a common picture of the battlefield has been a goal of commanders since armies have existed. Today this common picture is often associated with an image on a computer screen or with the product of a particular information system. However, each warfighting commander's opinion differs on what information should be displayed. The question then becomes, which common picture is common to everyone on the battlefield?

It is necessary to reexamine the definition of the common picture of the battlefield. The common picture is the sum total of information available within a predefined battlespace. Each commander will tailor that picture to meet mission needs and personal preferences. For example, the items presented on a maneuver commander's C2 display will differ significantly from that of an artillery commander's display even though they are concerned with the same battlespace. The common picture of the battlefield is not the information presented to the commander on a computer screen. Rather, it is the underlying database from which the image was presented.

Commanders must insure that the raw information is the same for all commanders and their staffs within the same battlespace. In order to achieve this goal, a common "information pool" is required from which all warfighters can extract information. A generic user terminal could then be created to provide access to all information available. This generic terminal would enable commanders to simultaneously display various items of information, regardless of Battlefield Operating System (BOS). For example, a brigade commander could display both friendly and enemy force dispositions along with air defense coverage, obstacles, and significant logistical considerations. It would not be necessary to present a series of overlapping overlays, making it difficult to pick out items of immediate concern. Figure 5 represents a conceptual information pool.

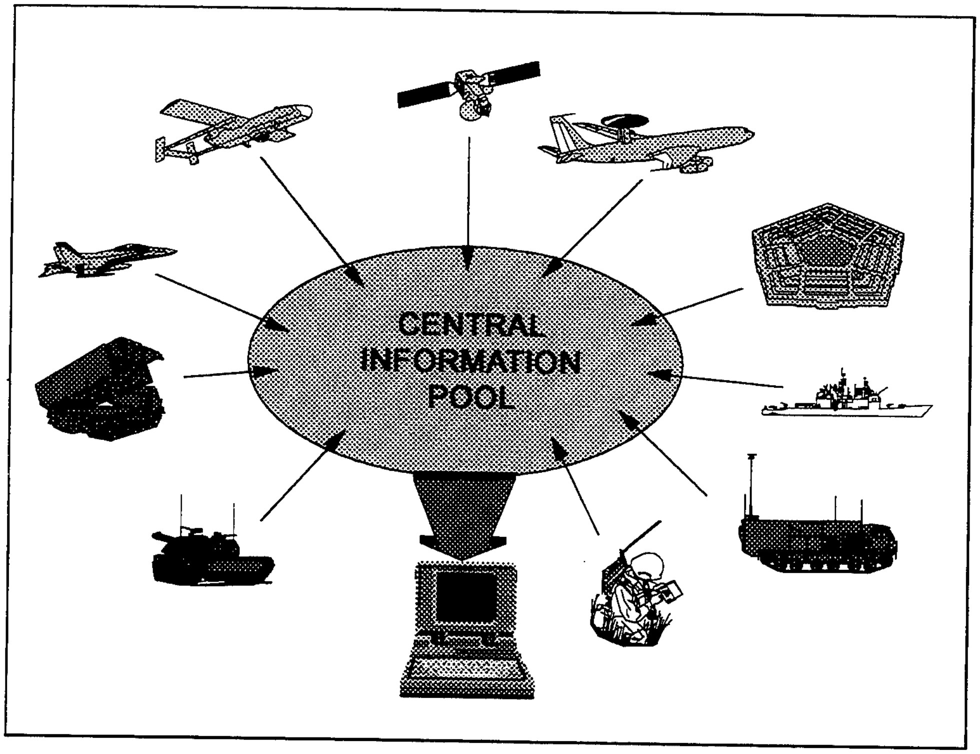

Figure 5. The Common Information Pool

Battle Staff. One of the greatest impacts of information technologies should be seen within the battle staff. Battle staffs are currently organized to support the various battlefield operating systems and are organized along traditional lines. As information begins to flow horizontally in an unrestricted manner, battle staffs will be able to manipulate and display information from a number of battlefield operating systems simultaneously. It then becomes possible to drastically reduce the size of the staff and substantially reduce the decision making time for the commander.

Security. System security will become of paramount importance as information sources are linked together. The intelligence community has commonly employed compartmentalization as a technique to limit unauthorized access to sensitive information. The creation of a contiguous information pool is in direct opposition to this technique. It therefore becomes critical to limit access of information within the common pool. Duty position could be used to identify and limit a given users access to the information pool. For example, a supply clerk in a company motor pool would have access to only that information which is necessary to carry out motor maintenance operations. Conversely, a Division Commander would have access to all information within his area of interest, to include that of the higher headquarters as required.

Importance

It is of vital importance that the Army establishes a clear picture of the information capabilities that will be required in the future. A comprehensive information architecture should be developed that will support Army Operations and leverage the best capabilities that information technologies have to offer. The Army's future information architecture must be developed with a two pronged development strategy. The first pronge takes a bottom-up approach, defining user requirements. Once a set of user information requirements are determined, the second pronge of the development startegy should be focused on developing an information network from the top-down, leveraging the best commercial technology has to offer in the most efficient network configuration. This approach creates unity of effort in the development of the objective information architecture. A fully integrated information network will provide the commander and his soldiers the ability to decisively win on the battlefields of the twenty-first century.

---

[1]Chairman, Joint Chiefs of Staff, C4I for the Warrior (Washington, D.C.: US Government Printing Office, June 1992), pp. 1-4.

[2]Director of Information Systems for Command, Control, Communications and Computers, Army Enterprise Strategy...The Vision (Washington, D.C.: US Government Printing Office, 1993), p. 2-6.

[3]Headquarters, U.S. Communications Electronic Command, Command, Control, Communications, Computers, Intelligence, and Electronic Warfare (C4IEW) Project Book (Ft. Monmouth, NJ: CECOM, 1995), p. 8-1.

[4]Ibid., 7-1.

[5]Ibid., 2-1.

[6]Ibid., 1-5.

[7]Ibid., 4-1.

[8]Director of Information Systems for Command, Control, Communications and Computers, Army Enterprise Strategy, (Washington, D.C.: US Government Printing Office, 1994), p. 2-7 - 2-8.

[9]Ibid., 2-10.

[10]Zysman, George I., "Wireless Networks," Scientific American, (New York, New York: Scientific American, September 1995), pp. 69-71.

[11]Ibid., 71.

[12]Directorate of Combat Developments, Modeling and Simulation ADO Study, (Fort Gordon, GA, 1996), p. 24.

[13]Maes, Pattie, "Intelligent Software," Scientific American, (New York, New York: Scientific American, September 1995), pp. 84-86.

[14]Lenat, Douglas B, "Artificial Intelligence," Scientific American, (New York, New York: Scientific American, September 1995), pp. 80-83.

[15]Headquarters, Department of the Army, Field Manual 100-5, Army Operations, (Government Printing Office, Washington, D.C., 1993), p. 2-0 - 2-9.

[16]Beam, Walter R., Command, Control, and Communications Systems Engineering, (New York, New York: McGraw-Hill Publishing Company, 1989), p. 1-11.

CHAPTER 3

OBJECTIVE INFORMATION ARCHITECTURE

Introduction

According to the Tofflers in their book, War and Anti-War, the world is undergoing a revolution. The current revolution is called the Third Wave. This Third Wave is based on the transition from industrial societies to knowledge based societies. Corporations are making the painful shift from hierarchical, bureaucratic, industrial organizations to distributed, specialized, knowledge based organizations. The U.S. Army has also begun this painful transition. Modern weapon systems rely upon automation to target and deliver precision munitions. This same principle should be applied to the warfighting commander and his staffs. The Army must step out of the box, examine both command and staff functional requirements and determine which functions are best suited for automation. The next step is to determine the optimal organization for a battlefield information network. Once this optimal information architecture is agreed upon as the blueprint for Army automation, the Army must focus its efforts and resources in attaining this goal.[1]

Standardization Efforts

Army Technical Architecture. The joint services have taken a number of steps to achieve a level of interoperability through the introduction of standards and guidlines. These standards cause developmental efforts to meet interoperability standards at all levels. Once such effort is the Army Technical Architecture (ATA). The ATA provides a starting point for the unrestricted movement of information and interoperability at all echelons, to include the sustaining base. The architecture establishes standards and guidelines for system development and acquisition. The ATA should greatly reduce cost, development time, and fielding time for any information system. The ATA defines a minimum set of rules that governs the arrangement, interaction and interdependence of the parts that together can be used to form information systems. The ATA is analogous to a set of building codes for construction. It does not dictate what is to be built or how to build it. It establishes the standards that must be met to ensure efficient operation. The ATA applies to all systems that will generate, store, use and exchange information.[2]

The second standardization effort is the Common Operating Environment (COE). The COE provides a reusable set of comon software services. Through the use of COE services, developers can focus their efforts on building functional area applications rather than replicating information service software. Figure 6 depicts the COE.[3] The COE is defined as a four layer architecture. Each layer segregates the functions of the lower layers from those of the higher layers in order to facilitate the insersion of new hardware or software without breaking the fundamental structure.

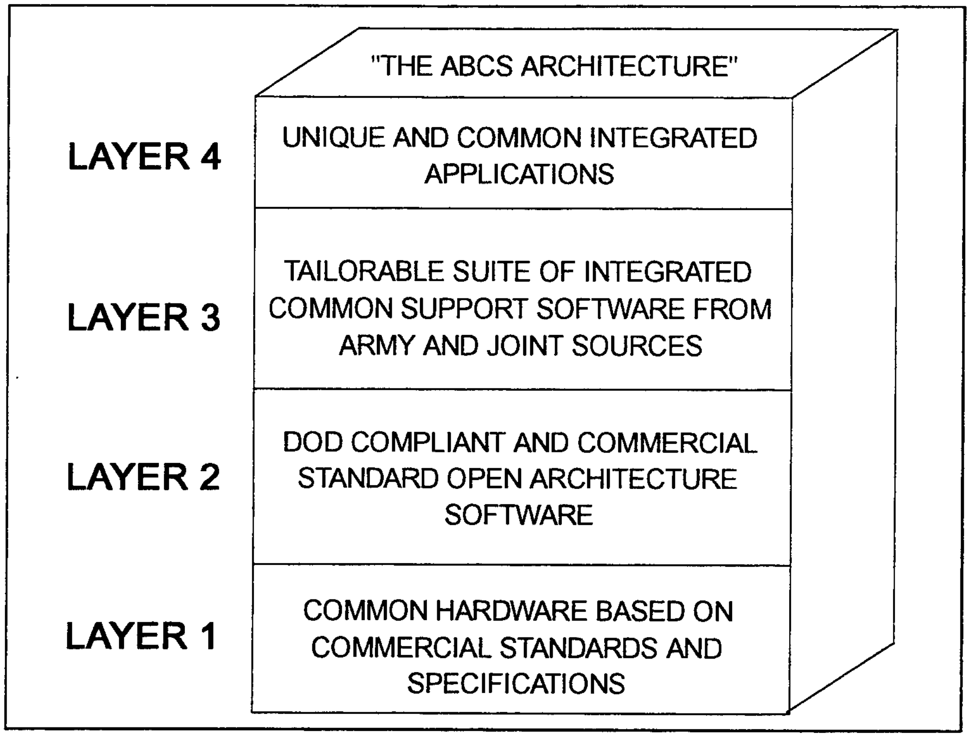

Figure 6. The Army's Common Operating Environment (COE).

Layer 1 decribes the hardware to be used in the architecture and the communication interfaces which must be provided. Layer 2 describes the required system support software. This software includes, but is not limited to, the operating system, database management system, and word processor. Layer 3 is the main component of the COE. It describes all application support software that provide the capabilities which are inherent in any application software. It defines that software which may be reused in various user specific applications. Layer 4 defines the unique user application software which is designed to meet user requirements in each functional area.[4]

Requirements

Commander's Impact. Any information architecture must be able to positively impact the commander's ability to orient, observe, decide and act. The majority of the commander's planning time is spent by the staff. The Army must therefore focus on the ways to leverage automation so that the majority of the commander's planning time is spent on deciding and acting, not gathering information and conducting a thorough analysis. The Army must never lose sight of the fact that command is a combination of art and science. While it is generally true that the science of command can be automated, it is impossible to automate the art of command. The art of command enables each commander to create unique solutions to tackle unique problems. Commanders must be freed to exercise the art of command. Figure 7 depicts the Military Decision Making Process. This manual process will serve as the baseline for all future discussion regarding the capabilities that should be provived by an information network to shorten the commander's decision cycle.[5]

The staff actions listed on the left side of figure 7 represent the majority of time expended during the decision making process. Specifically, the staff estimate is focused on gathering information, whether by data message or voice, and providing information products to the commander. The commander then uses this information to perform mission analysis and to issue planning guidance to the staff. The process of gathering information and placing it in a usable format represents the science of war and is extremely time intensive.

Current information solutions tend towards replicating antiquated staff processes, such as the military decision making process, and do little to reduce the commanders decision cycle. Warfighting commanders as well as their supporting commanders must be able to readily access automated staff products simultaneously, in near real time.

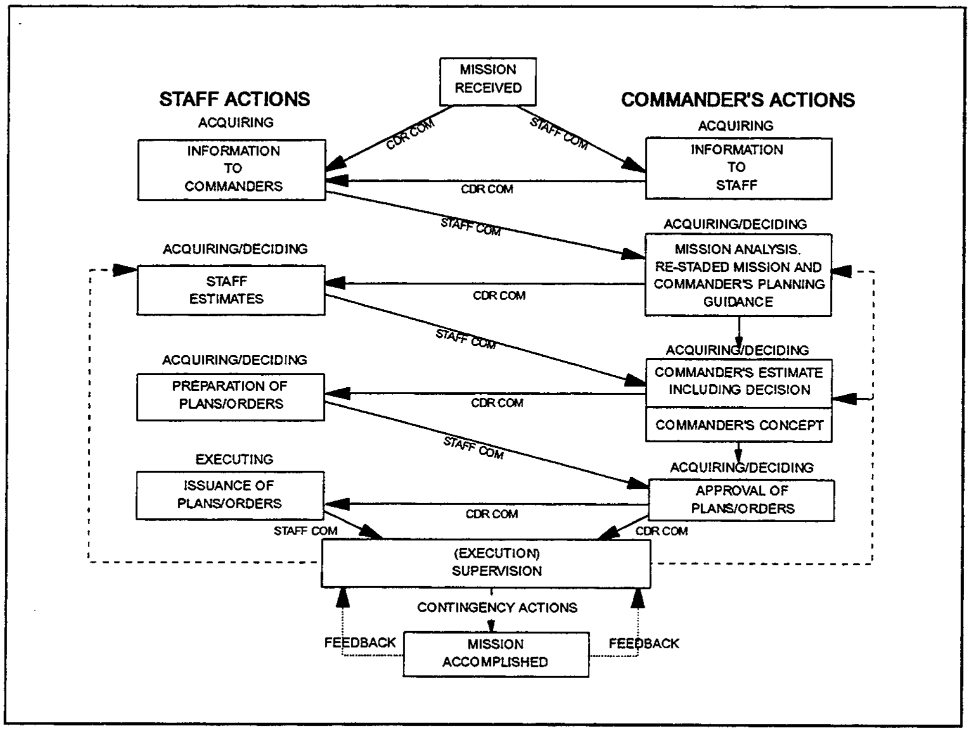

Figure 7. Military Decision Making Process.

A commander must be able to preselect critical information requirements and be able to rely on an information network that will supply him with the necessary information to decide and act. The information must be intelligently pushed to the commander. A commander should never be required to look through files, sort databases, or "surf a web on the Internet." These are all time-consuming processes which will only hinder the commander.

The network must also be highly responsive to the commander's requests for additional information. The information should be produced on demand in near real time and the commander should be alerted when the information is available. This requirement demands a network that is both highly flexible and responsive.

"Knowledge-based" Staff Functions. A high performing battlestaff, as described by Lieutenant Colonel Henry L. Thompson, is a highly dedicated, cohesive, and innovative battle leadership team that is made up of commanders, their staffs, and their subordinate commanders. This battle leadership team must develop synergy if it is to achieve high performance. Synergy is the total effect created by the combination of all of the efforts of the group. This effect exceeds the sum total effect of the individual efforts. Synergy is achieved through integration between echelons within a single Battlefield Operating System (BOS) and through synchronization among all the BOSs. Integration and synchronization must occur if synergy is to be achieved. The information architecture should facilitate commanders and staffs in achieving synergy.[6]

Gather Information. Once a commander has provided guidance to his staff regarding a particular mission the staff begins to gather information or facts bearing on the assigned problem. Requests for information are sent to subordinate staffs which in turn also gather information. Information bearing on the problem comes from a wide variety of sources and requires numerous messages, phone calls, and radio transmissions. Staff procedures such as scheduled reporting relieves some of the burden, but represents a relatively small portion of the information to be gathered. This process tends to be extremely time consuming.

The benefits of an information network to support the gathering of information are readily apparent. Vast amounts of information from a wide variety of sources may affect a commander's decision. Any information network must be able to accept large amounts of information from across the battlefield regardless of BOS. It is vital that any piece of information is input to the network only once. An information system that requires only one input to produce multiple actions reduces the possibility for error and decreases the number of actions to be taken by system users. This approach results in reduced communications, saved time, and saved labor.

Stovepiped systems are those automation systems that are designed to support only one function. Stovepiped systems are uniquely developed and lack interoperability with other automation systems. Current information systems tend to be stovepiped and require multiple inputs of the same information for each system. For example, when a soldier is killed in action a significant number of actions are initiated. First, the loss must be reported to higher headquarters since the information impacts on the unit's combat effectiveness. This information must be provided to a command and control system. Second, the personnel system requires this information so that a replacement can be identified. This requires a second input. Third, a finance system must be informed so that the appropriate pay actions can be initiated.

Fourth, the state-side unit must be informed in order to ensure casualty notification occurs and survivor benefits are initiated to provide proper support to the soldier's family. There are many more actions which must occur, but it is clear that a single event requires multiple inputs of the same information. See Figure 8.

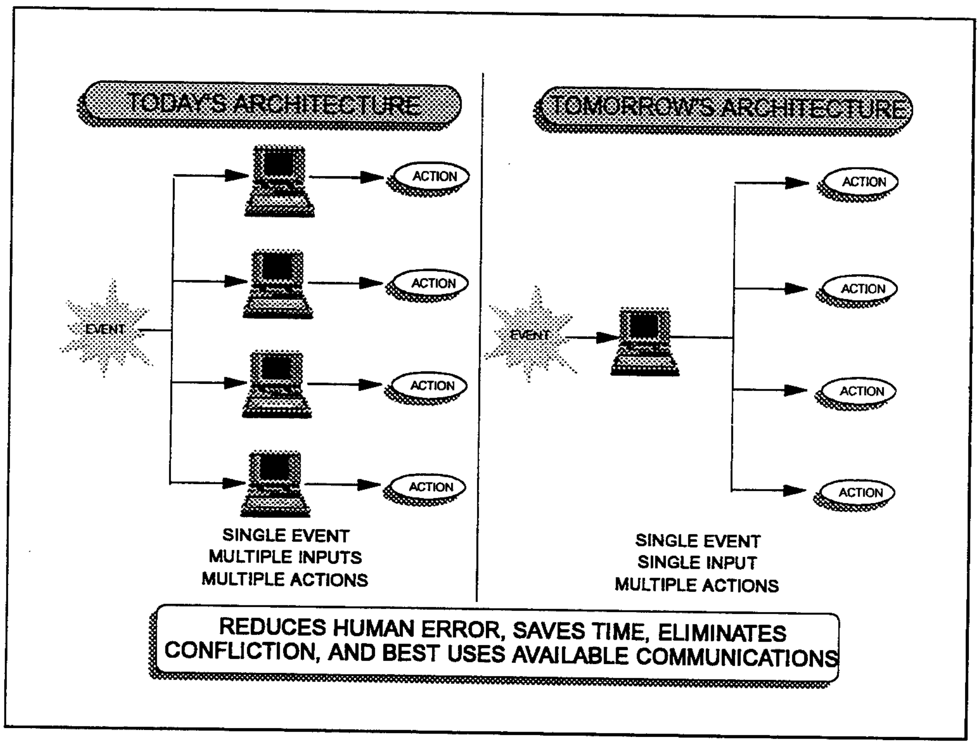

Figure 8. Reducing Human Error.

An Army-wide information network must permit a single input for a single event. Staffs at all levels should be able to access that information at any echelon, in any format.

<u>Process and Analyze Information</u>. The next largest portion of the staff's time, and hence the commander's, is dedicated to processing

and analyzing gathered information. The staff must first process the information into a usable format that will facilitate analysis. This is done by creating tables and charts and a great deal of number crunching. Once the information is in a digestible format, each staff member is able to apply the art of their specialization to the problem.

The actions involved in processing information readily lend themselves to automation. The information network must be able to independently process raw or "base level" information into the appropriate format. This processed information must be readily available to the staff so that they can apply the art of analysis to the problem. The resultant analyzed staff products can then be input into the information network where it would be available to the commander and his entire staff. The staff can then focus their time doing innovative thinking, rather than redundant and mundane information gathering and processing.

Presentation. Based on this conceptual model, the information network provides the commander three levels of products; base-level information, processed information, and analytical information products. The information resident at each level must be available to the commander and staff in near real time. Figure 9 depicts the Tiered Database Model. Any user should be able access any and all pertinent information, provided access is authorized, and integrate it into a single display. The single display must be tailorable to each commanders unique needs and preferences. It should not be a series of overlapping overlays with extraneous information. Various items of information from each BOS must be able to be selected for presentation and integrated into a single presentation.

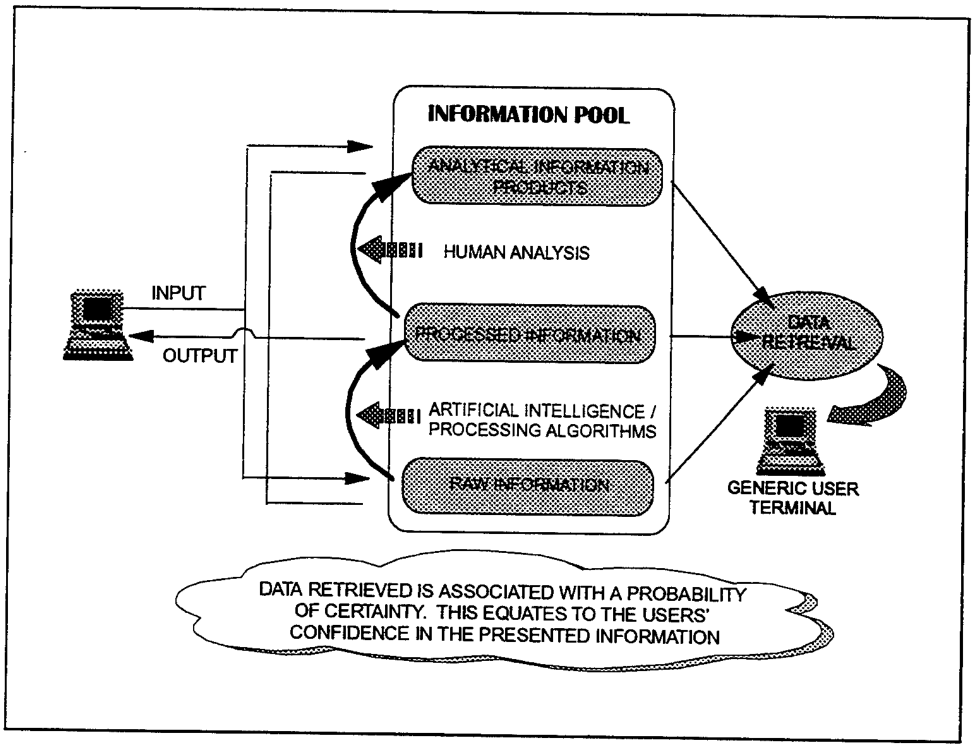

Figure 9. Tiered Database.

Additionally, the information network should be intelligent enough to seek out information based on preselected criteria. This criteria should conform to the Priority Information Requirements (PIRs) of the unit. PIRs identify that information which is deemed important by the warfighting commander to the success of the current mission. Each user must have the capability to determine which information is fed to their local terminal. Once the information becomes available, the system should automatically alert the user of its presence and present it. For example, a Task Force commander has a mission to conduct a raid to secure a bridge in the enemy's sector. Seizure of the bridge will support the division's main effort during the current operation.

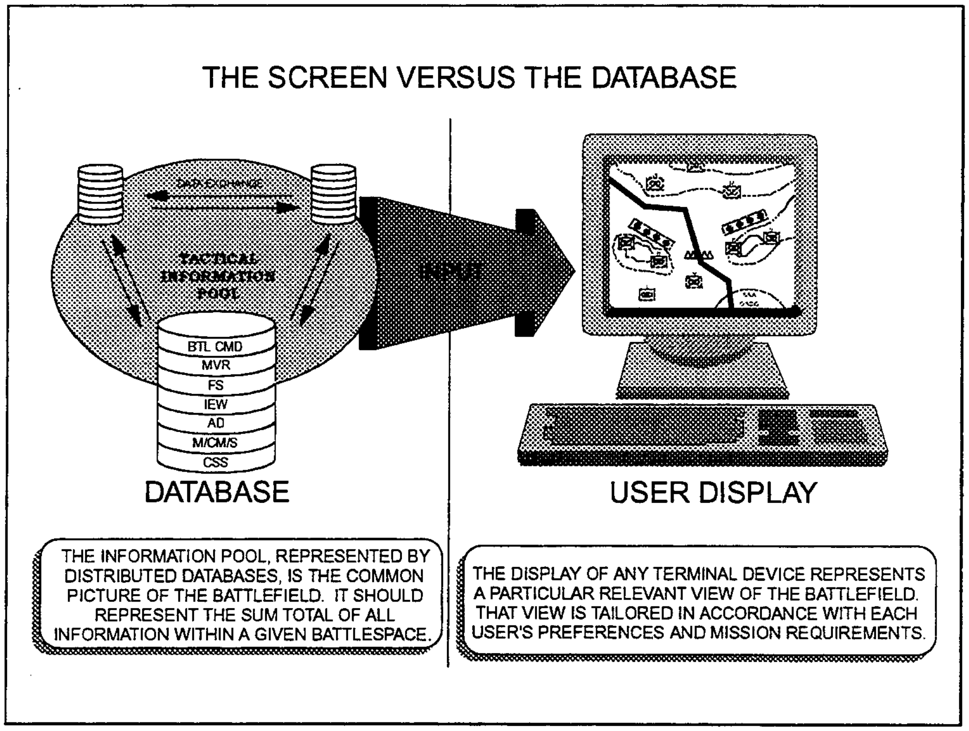

Figure 10. Common Picture of the Battlefield.

The task force commander would be able to tell the information network to inform him, and those he selects, that in the event that friendly forces detect the destruction of the bridge, he be informed immediately. Friendly intelligence assets, directly feeding the information network, could then detect and report the destruction of the bridge. The information network would then recognize that this was information that a specified Task Force commander required. The information would then be automatically transferred to the commander's terminal. An icon could appear with an audible alarm or synthesized voice informing the commander of his objective's destruction. He would then exercise the art of command and select a secondary objective that fit within the division commander's guidance.

Support the soldier. Any information network developed must keep the soldier foremost in consideration. The soldier in the field is the primary generator of information into the information network and the ultimate recipient. Infantrymen at the tip of the spear, soldiers manning JSTARS terminals, logisticians tracking supplies, signal soldiers linking command posts and medics saving lives are all the most vital link in the information chain. They ultimate determine which information is provided to the common pool of knowledge that the commander will rely upon to win the next war. Figure 11 depicts a BOS immaterial user display.

It is critical that the soldier's user device presents the most accurate and timely information available. The generic user terminal must consist of a common hardware baseline. The user interface must be the same, regardless of the desired function, facilitating the ease of use. Any terminal must be capable of rapid reconfiguration by the user, with a set of user system preferences that would be loaded with a minimum of effort. This means that any terminal could be used by any user regardless of that users specialty, MOS or function. For example, if a logistician picked up an infantryman's terminal device, he could reset the terminal's user parameters and immediately commence to accomplish logistic tasks without being required to load unique BOS and user interface software and establish unique point to point communication paths.[7]

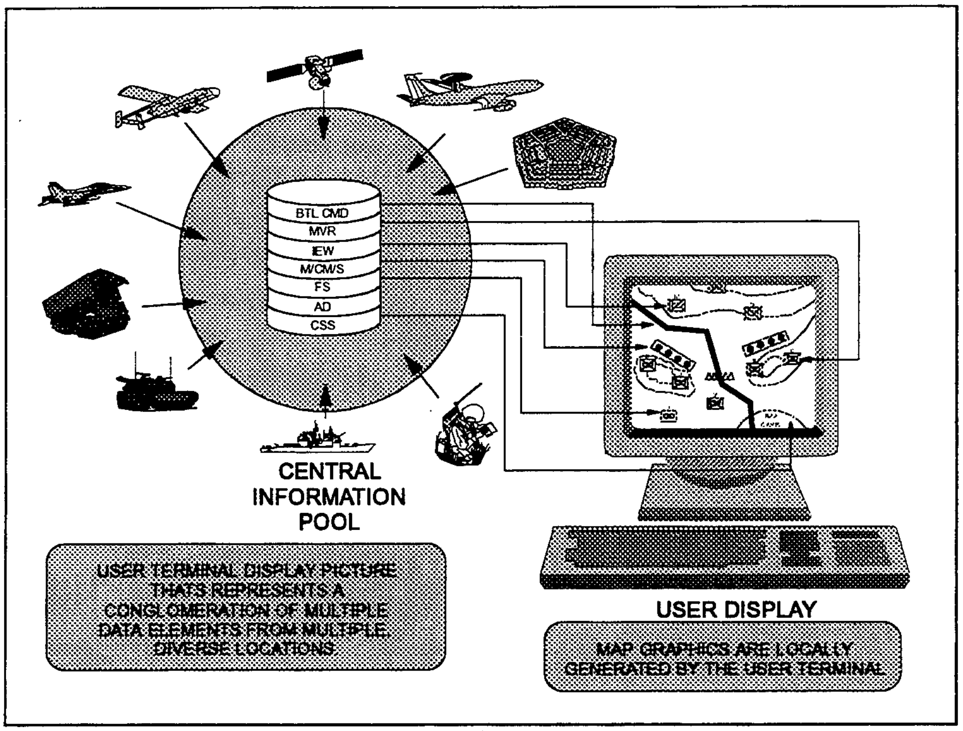

Figure 11. Displayed Objects Retrieved from across the Information Pool.

Mobility. Every warfighting commander recognizes that mobility is critical to success on the modern battlefield. Mobility provides the commander the capability to outmaneuver his opponent on the battlefield. It provides him the ability to attack exposed flanks and wreak havoc in the enemy's rear; critical components to success. The proposed information network must recognize this requirement, since information is the key to the commander's ability to effectively maneuver friendly forces. The scheme of maneuver is essential, in providing situational advantage, relative to the enemy and the capability to mass combat power at the decisive point.

It is important here to recognize that there is an inverse relationship between information requirements and mobility. As the information requirements of a particular location, whether it is a Division Tactical Operations Center (DTOC) or an M-1 tank, increases its mobility decreases. This is based upon the physical limitations of communications. An increase in the requirement of timely information at the TOC demands an increase in the size and complexity of the communication transmission system is required. For example, the SINCGARS radio system is highly mobile, but its capability to receive and transmit large amounts of data is limited. The MSE system can transmit much larger amounts of information, but the system is much less mobile than SINCGARS. Figure 12 represents the relationship between information demand and communication mobility. The figure also depicts where current communication systems fall within the relationship.[8]

Every information user is tied to the communications that supports him. A TOC can be no more mobile than the communications that supports it. It is therefore necessary to design an information network that meets both the information and mobility requirements of the soldier. In preliminary examination this appears to be an unsolvable dilemma.

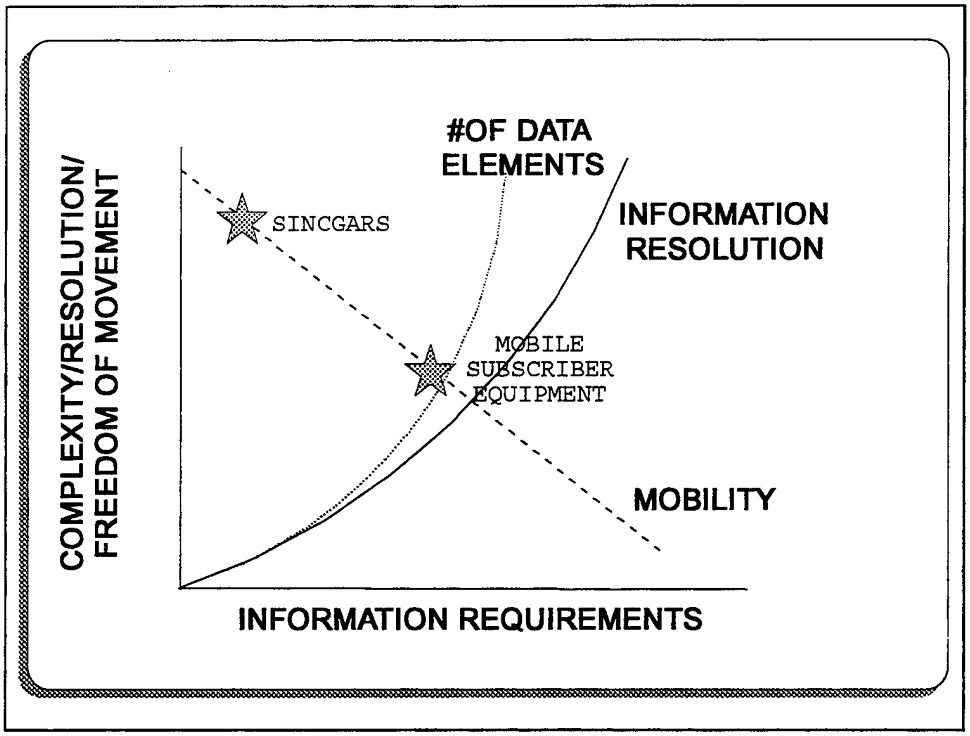

Figure 12. Information Transmission Requirements versus Communication Capacity.

The answer lies in the efficiency of the information transmitted. An information product, or an answer to a commander's question, requires far less transmission space than all the data required to generate that answer. An efficiently packaged information product requires even less communications support. The less communication support required means increased mobility for the warfighter. We can then conclude that it is in best interest of the soldier to create efficiently packaged information products in an information pool rather than at the user's location.

Protection. Each commander must be able to rely upon constant communications with the information pool. This can be accomplished with multiple, redundant, highly reliable communication paths and information access points. A variety of communications means must be available to all users at a given location along with multiple access locations. Additionally, the process of selecting the communications means and the access point must be rapid, efficient, and transparent to the user.[9]

When propeller driven ships were first commissioned in the U.S. Navy, sails were included in the design. The sails were eventually removed once the propulsion systems became much more reliable. The same will be true as the Army transitions to a knowledge based force. Reliability will have to be proven before commanders will let go of the systems of the past.

Controlled Access. Commercial industry has recognized that the protection of a computer based information pool is essential. This same requirement must be placed on the Army's information network. It is insufficient to limit user access to a given security level. The Army must address the requirement for controlled access; the user's need to know. The Army must recognize the fact that granting a soldier access to a level of classified material does not mean that soldiers should have access to all the information available at that classification level. We must therefore be able to control the user's access to information.[10]

Creating an information pool simplifies this process. A single, virtual information pool facilitates a single solution for controlled access. Each entry point within the information pool must implement a security solution. Once access has been verified at the entry point, the user is then permitted to use information throughout the information pool providing that the user's need to know has been previously established.

---

[1]Toffler, Alvin and Heidi, War and Anti-War, (New York, New York: Little, Brown and Company, , 1993), pp.18-25.

[2]Department of the Army, C4I Technical Architecture, (Washington, D.C.: Government Printing Office, 1995),p. 2.

[3]Headquarters, Department of the Army, The Common Operating Environment, (Washington, D.C.: Government Printing Office, 1994), p. 6.

[4]Ibid., 5-7.

[5]Thompson, Henry, LTC, "The High Performing Staff", Army Organizational Effectiveness Journal, (Washington, D.C.: Government Printing Office, 1984), pp. 6-7.

[6]Ibid., 2-5.

[7]Headquarters, U.S. Army Training and Doctrine Command, Operational Requirements Document (ORD) for Army Battle Command Systems (ABCS), (Fort Monroe, VA: Government Printing Office, 1993), p. 1.

[8]Directorate of Combat Developments, Modeling and Simulation ADO Study, (Fort Gordon, GA: United States Army Signal Center, 1996), pp. 17-18.

[9]Ibid., 2.

[10]Center for Information System Security Defense Information Sytems Security Program, Department of Defense Goal Security Architecture, Version 1.0, (Maryland: Government Printing Office, 1993), p. 2.

CHAPTER 4

THE ATHENA NETWORK: TRANSFORMING THE ARMY

Athena: An Architectural Solution

Any architectural solution must be designed in such a way that will allow the warfighting commander to focus on decisively defeating the enemy. Warfighting requirements must be kept paramount in the design of any information network. This fundamental requirement will place large demands upon signal soldiers across the battlefield. The Signal Corps is the Army branch best prepared to assume the role of battlefield information manager, however the current signal mission must be redefined.

The following proposed information architecture has been named Athena after the Greek goddess of wisdom. In Homer's Iliad, Athena is described as a fierce goddess of battle who repeatedly intervened during the Trojan War in favor of the Greeks. As the goddess of wisdom and knowledge, particularly in warfare, the name Athena appropriately depicts the goal of this information architecture; to provide the warfighting commander with the required information to win on the modern battlefield.[1]

Information Pool. The formulation of a responsive, survivable information pool will be critical on the future battlefield. The concept of an information pool can be derived from the trends currently seen in commercial research and development efforts. Commercial industry has recognized the limitations imposed by terrestrial and space based communications and has begun to examine the potential of distributed databases, data mining, and distributed data processing. Currently, most commercial industries employ a client-server architecture which supports user applications. The user requests and receives information from a single server that is interconnected to other servers. Information that is passed from distant servers to the local server is not processed. It is forwarded as complete files of information, regardless of the user's request. The burden then falls upon the user (client) to filter the unwanted information from the desired information.[2]

This architectural design is predominant today, but leaves little room for growth due to the inefficient use of the available communication means. The goal of commercial research and development efforts is to create a distributed information network which will appear to the user as a single information pool. Clear trends towards open, distributed, object-oriented computing have been well established. This is readily apparent in the R&D efforts of the GTE and CWI Corporations which are major information service providers.

Any information architecture that will support command and control requirements must recognize this industrial trend. Tying the Army's information architecture to this well defined industrial effort will ensure the Army maintains the ability to leverage commercial technology well into the twenty-first century.

Distributed Databases. Major information service providers, such as GTE and CWI, have all stated that the development of distributed information networks will be vital to maintain their competitiveness in the world market. Research and development efforts have been focused towards solving the problems inherent in a distributed network. GTE efforts have focused on the goal of creating a network that allows all resources available in a distributed network to function as a commonly-accessible collection of objects which can be combined in unique ways. This would potentially lead to new information processing capabilities.

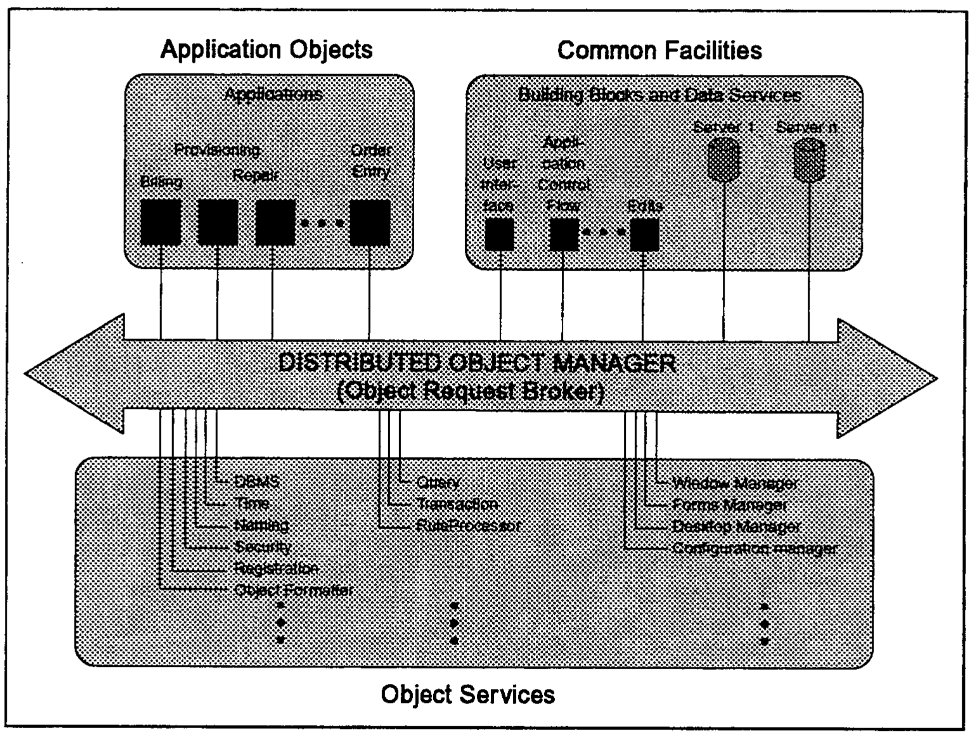

Figure 13. GTE Distributed Object Management.

The GTE application framework, depicted in Figure 13, describes an architecture for a global network of heterogeneous, new and legacy information systems. The effectiveness of the operation of an individual system will be heavily dependent upon the interoperability of all systems. The GTE framework defines a possible distributed object management technological solution. The model views all elements within the network to be treated as a "commonly-accessible collection of objects." The distributed information network employs varying applications (billing, repair, order entry, etc.) that are connected to the Distributed Object Managers (DOMs) that support seamless interoperation. Users at common facilities process information through transparent interoperation, coordination of application objects, and the use of available object services.[3]

Distributed Processing. The greatest challenge in developing a distributed information network is the ability to locate information across the network and the means to process that information. Industry is examining a number of techniques to solve this problem. Data mining is the search for patterns and relationships at the global level. These patterns exist in large databases, but are hidden among the cast amounts of information. Data mining research is focused on developing intelligent search patterns to detect global patterns. This technology will rely heavily upon statistical analysis to determine the reliability of located relationships. Once the applicable information has been located, the appropriate processing algorithm(s) can be applied by the network to create the desired processed information product as described in Chapter 3.[4]

Capabilities. It is important, at this stage, to describe the capabilities that the Athena information pool must provide if it is to serve the needs of the warfighter. Keeping the required capabilities in the forefront of the architectural design will ensure the development of an information network that is reliable, redundant, survivable, and supports highly mobile users.

Redundancy. An information system with this degree of complexity will require redundancy to ensure reliability. Each information node within the architecture must provide a backup capability to increase the reliability of the node. This can be accomplished by providing one hundred percent backup on all critical systems. Additionally, the system should also provide an archiving capability to facilitate retrieval of previous events. This information will be critical in developing likely enemy courses of action based on past experiences and in the summation of lessons learned once a mission has been successfully accomplished.[5]

Reliable Access. The Athena information architecture causes the warfighter to be physically separated from the information critical to success on the modern battlefield. It then becomes of paramount importance to ensure reliable access to the tactical information pool. This can be done by two methods. The first is to develop communication systems that achieve a high degree of reliability in a combat environment. Acquisition of current communication systems are continuously focused in this area. Secondly, the warfighter must be provided multiple communication means to ensure continued contact with the information pool. Multiple communication means should include the appropriate mix of satellite, terrestrial, tactical and commercial systems. These system should then be tied to a communications server, a device that will automatically select the best communications path to the information pool based on the location of the warfighter and the type and amount of information requested.[6]

Survivability. Force and C2 Protection are two issues that are a major concern of today's Army. As the Army moves into the Information Age, protection of automated C2 systems will be a significant concern. Any potential enemy will understand the criticality of C2 systems to U.S. Army operations. Athena's distributed database network must be designed to ensure it can survive both physical and electronic attacks. This can be done by replicating information contained in one information node at multiple adjacent locations. This will ensure that the loss of an information node does not equate to the loss of information. Database replication between information nodes must be automatic and timely. This requirement must be weighed against the communication assets available to preclude a backlog of information at any given node in the network.

The user end of the network should also take into account the potential destruction of the information node that is providing access to the tactical information pool. Automatic system reconfiguration is an essential element in the design of the information architecture. If an information node is destroyed, user access should be automatically transferred to the nearest adjacent node. This must be accomplished automatically and appear transparent to the warfighter.

Mobility. Mobility and allowing the warfighting commander the freedom to maneuver forces will be critical on future battlefields. The Athena information architecture must support this principle. The warfighting commander should never be tied to the information system in order to exercise command and control. It is this principle which drives the development of the two tiered architecture; information nodes and user terminals. The complexity of the network is placed at the information node, not the user terminal. The warfighter's generic user terminal and the communications to support it must be as mobile as the user. The information network, as a whole, must therefore support automatic reconfiguration. Reconfiguration should include automatic access to an available information node, automatic selection of the best available communications path, and automatic network adjustments based on the movement or destruction of information nodes.

Controlled Access (Security). Increased reliance on automated C2 systems increase the U.S. Army's vulnerability to attack. Future enemies will perceive our information networks as one of our centers of gravity and will ensure their warplan includes its attack. Enemy efforts against our future C2 networks will include exploitation. Potential enemies will seek the means to penetrate our information networks and exploit the information contained within. It is therefore vital that access to the tactical information pool of Athena be controlled. Current efforts are designed at separating the levels of security between unclassified, secret, and top secret. Additionally, increasing interoperability among the various Battlefield Operating Systems (BOS) also increases access to any user once the system has been entered. Therefore, once access to a particular security level is granted, a user is free to access information throughout the network.. This approach does not address the long standing requirement to limit the information provided to only that which a particular user needs to know.[7]

Athena's tactical information pool must be capable of limiting access based upon a user's need to know. Security of the network can be achieved by designating an access code to each system user. The access code would be verified by the network prior to the release of any information at a given information node. The access code could be initially tied to the user's job position. For example, a supply clerk would have very limited access to the information available within a division's tactical information pool. Conversely, the division commander would be granted complete access to all the information available in the division's informational pool. In a sense, a cover would be placed over the available information and based on a given user's access code the cover would be raised from those items of information for which the user has been granted access. The commander would be the ultimate decision maker regarding which information should be made available to which subordinates. System administrators would then implement those decisions on the network. A number of biometric technologies are under development which would facilitate controlled access. These technologies will be discussed in more detail later.

Generic User Terminals. Supporting the needs of the warfighter will be paramount in the development of user terminals. A fundamental principle of the Athena architecture is that the complexity inherent in the network be placed within the infrastructure, not in the user terminal. Additionally, the software implemented on the user terminal for the battlefield should be the same as is utilized in garrison. This design permits warfighters to focus on the business of warfare, not on information management and training of unfamiliar software.

Capabilities. The family of Generic User Terminals (GUT) must provide a series of capabilities that will meet the diverse environments that will be found on future battlefields. GUT software must be common and support a wide variety of user applications. A user must never be required to learn new software packages each time a new terminal is accessed.[8]

Tailorable. Each terminal must have the capability to be uniquely tailored to meet the needs of a particular user. Rapid reconfiguration of a GUT is essential. This can be accomplished by establishing a set of user preferences. The preference set could then be stored on a "swipe card" similar to that used by most credit cards. A user would no longer be tied to a specific device. A card reader would be provided with each terminal. The user would then "swipe their preference card through the reader. The GUT terminal would then automatically reconfigure itself to meet the needs of the current user. Reconfiguration would include, but not be limited to, display presentation, file organization, and mail accounts.

BOS Immaterial. Current C2 system configurations lock users to particular terminals based on the desired BOS. As previously stated, the warfighter should not be tied to a particular terminal device in order to accomplish a BOS specific function. The integration of information within Athena's tactical information pool enables the development of BOS immaterial user terminals. User devices can therefore be readily replaced and rapidly configured for use, regardless of the task.

Biometrics. Significant Research and Development (R&D) efforts are well established within the government and commercial industry. Technologies such as voice recognition, retina scans, and fingerprint recognition techniques are all being used in various industries and governmental agencies.[9]

Voice recognition technologies are of two types; user specific and user immaterial. User specific techniques are the simplest to implement since the system is required to recognize only one voice pattern. This technology readily applies itself to the requirement for controlled access. Unique voice patterns would have to be recognized by the network once access was requested. The Athena network would then compare the voice sample taken at the user terminal against previously validated samples. Once a match is detected, access is granted.[10]

User immaterial voice recognition technology is more difficult to implement because the GUT must be programmed to recognize a voice command regardless of tone, inflection, or regional accent. This technology requires a larger database of voice samples so that commands are accepted by a variety of users over a range of combat situations. Standard interfaces such as a keyboard or a mouse do not lend themselves to use in a moving armored vehicle or by an infantryman involved in a fire fight. Data entry and requests for information by voice command would be invaluable to the soldier. Although this technology presents challenges, the potential benefit to the combat soldier warrants investigation. Any GUT terminal should be designed to accept this technology as it becomes available.[11]

Retina and fingerprint scans provide another potential solution for controlled access. A peripheral device could be provided to verify a user's identification. Just as in voice pattern recognition, the sample taken would be compared against a database of known samples. Once a match is established, access is granted. User unique techniques such as those listed above represent a means to prevent enemy forces from using captured U.S. Army terminals. Without the proper user verification, the Athena network would deny access to any hostile agent attempting to break into the tactical information pool.

Regardless of the access mechanism employed, the system should provide each soldier the capability to enter a duress code. A duress code is an input intentionally entered by a soldier to indicate that he/she has been captured and is being forced to enter the network. Entering a duress code would have no apparent effect on the terminal unless it is desired that the terminal be shut down. The Athena network would also be capable of providing false information to the captured terminal in support of a deception operation. This choice would be up to the commander.

Configurations. GUT hardware must exist in a number of configurations to support a variety of Army missions. Commercial technology should be leveraged whenever possible, however warfighters must function in a variety of environments and most commercial devices will not withstand the rigors of combat. A mix of GUT types would represent the best approach to this requirement. It as an approach similar to that currently pursued under the Army's Common Hardware Software (CHS) program. GUT terminal types should be limited to portable, mounted, and desktop.[12]

Portable (military). The portable GUT terminal should be designed to support dismounted operations. Dismounted operations include those conducted by the infantry, the airborne infantry and special operations. This terminal type should be small, lightweight, and power efficient. It should be capable of operating in a variety of temperature extremes and ruggedized to accept the rigors of combat.

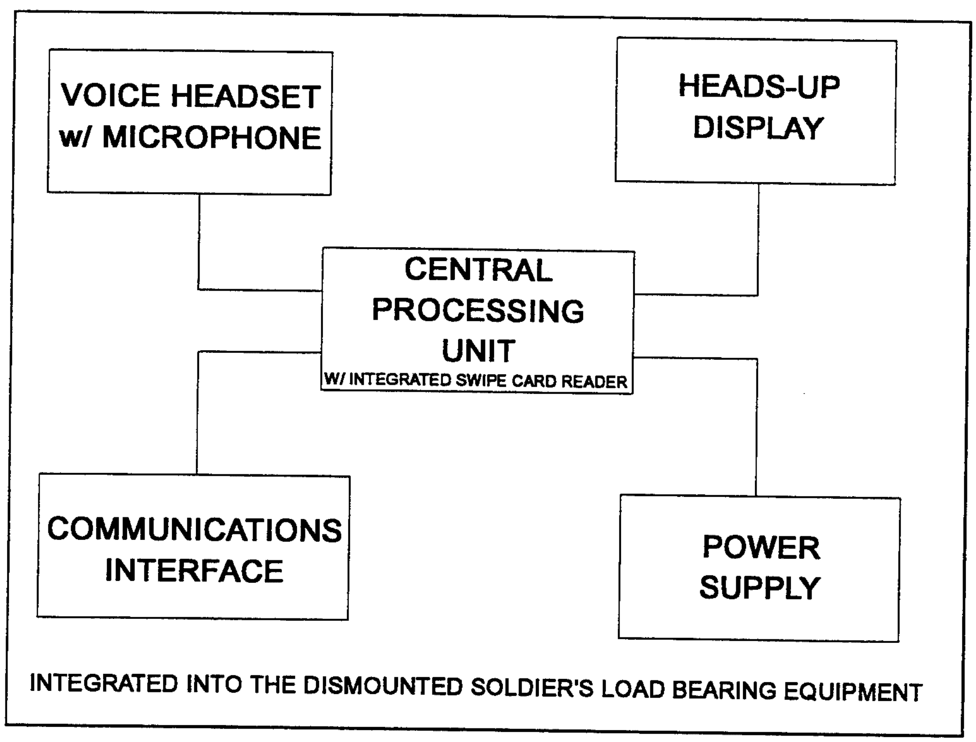

Figure 14. Portable Generic User Terminal (GUT).

The system must be designed as a component of a total soldier system. The total soldier system should incorporate the portable GUT, user interface devices (microphone, keyboard, visual display), communication assets, power supply, integration to the weapon system. The entire system should be integrated into the infantryman's Load Bearing Equipment (LBE). Voice recognition would be the optimal solution to meet the controlled access requirement as it will eliminate the need for peripheral devices. Figure 14 depicts the major components of the Portable GUT terminal.

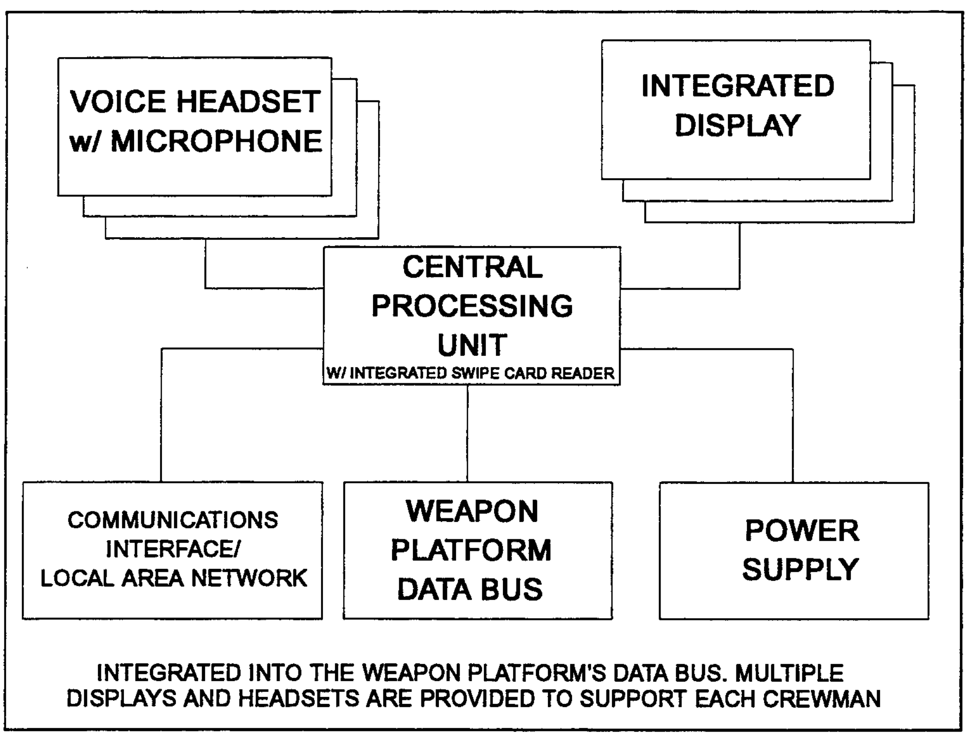

Figure 15. Mounted Generic User Terminal (GUT).

Mounted (military). The mounted GUT must meet the same set of requirements as the dismounted GUT, with the following exceptions. The weight of the terminal may be increased to support operations in an armored or wheeled vehicles. GUT interfaces should include those listed for the Dismounted GUT and include automated interfaces to the weapon system, all sensors, and weapon platform system status (fuel remaining, rounds on board, intercom, and any additional displays throughout the platform). Figure 15 depicts the Mounted GUT terminal.

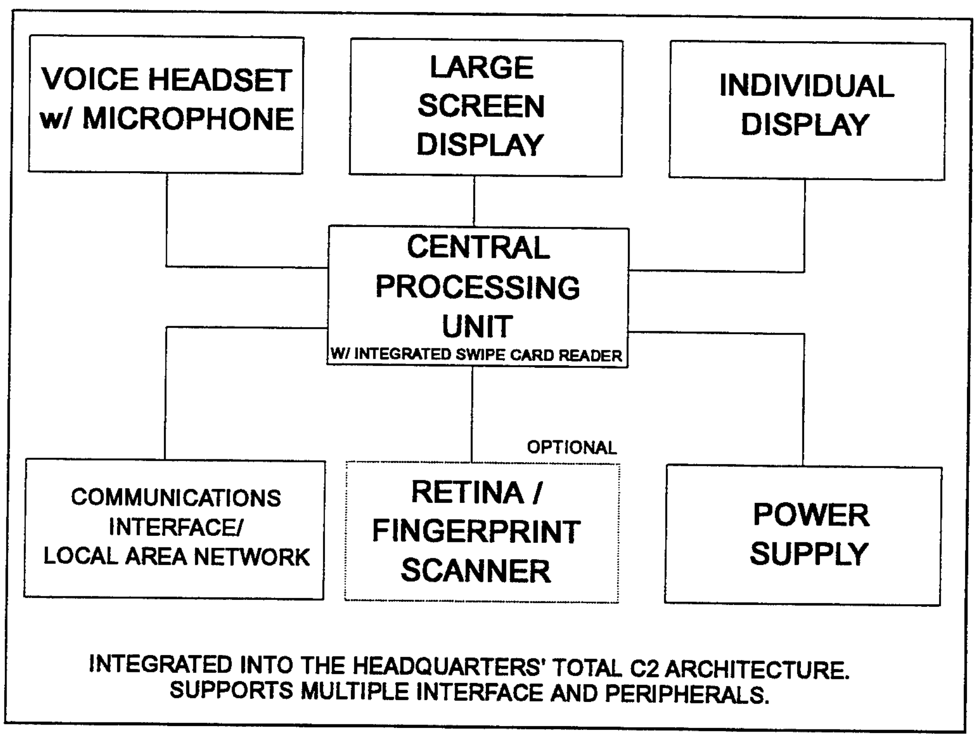

Figure 16. Desktop Generic User Terminal (GUT).

Desk Top (TOCs). The Desktop GUT is the version which will be found in most headquarters and garrison locations. This terminal will be the best candidate for the use of Commercial Off The Shelf (COTS) technology. Ruggedization requirements will be dropped favor of commercial options. The terminal must conform to the same capability requirements as outlined for the two previous terminals. Additional interfaces will include large screen displays, integrated and Video Teleconferencing (VTC). Figure 16 depicts the Desktop GUT.

Simulation Training. A side benefit of the Athena architecture is the use of the same software to support simulation training similar to that provided in the Battle Command Training Program (BCTP). The software could be reused at the Simulation Centers to train battle staffs either at the center or at home station through leased circuits. The warfighter would then be training with their own GUT terminal. The only additional requirement for the Simulation Centers would be to generate and input feeds that would normally be provided by weapon systems and battlefield sensors. Commanders and their staffs would then be able to develop their preference set for use in war and be afforded the opportunity to practice with it. At the end of the simulation, users will have loaded their updated preference set on their personal "swipe card" for use in the field. Warfighter would then be able to train as they fight.

Implementation

In order to implement Athena, an examination of the capabilities across the battlefield was conducted. My analysis focused on determining the optimal location for information nodes within the division AO. Athena information nodes consist of high-end, complex automation devices which act as information warehouses within the division. The seamless interconnection of these information nodes, or distributed databases, creates the virtual information pool. The largest communications requirement for the Athena architecture would exist between the information nodes as they share information throughout the network, ensuring the most current information is available.

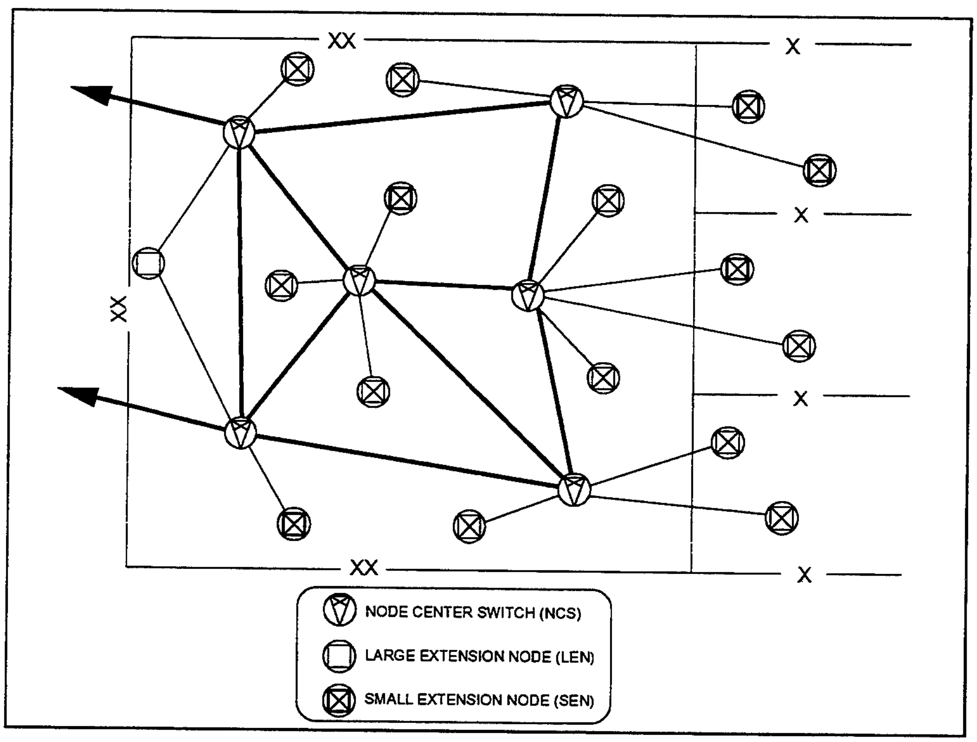

Figure 17. Mobile Subscriber Equipment Architecture.

Within the division AO, the largest communication paths exist between the MSE node centers, at 1024 kbps. The size of the communication paths via MSE decrease fron node centers to division headquarters (DTOC, DISCOM, DTAC, BDE Hqs, etc.) by approximately one fourth (256 kbps). Bearing this in mind, it is easy to see that the nodes of the MSE network provide the optimal location for the largest information nodes of the tactical information pool and the smallest within the maneuver brigade. Information nodes can then be divided between three types; large, medium, and small.[13] Figure 17 represents the MSE communications network, which must support the distributed information architecture.

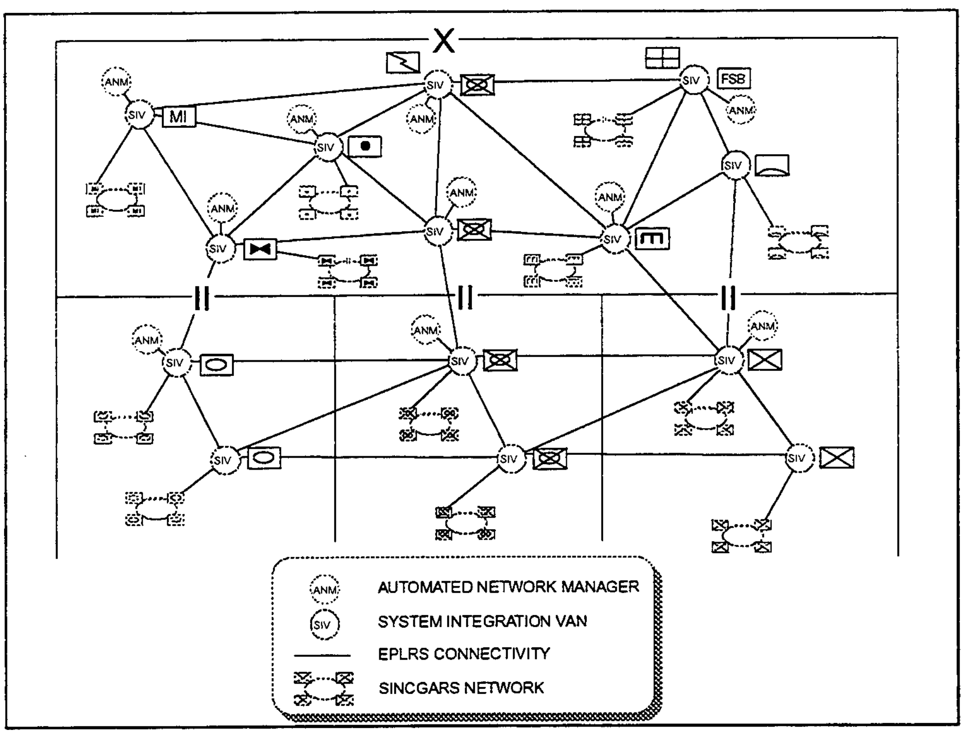

Figure 18. Tactical Internet Architecture.

Within the maneuver brigade, the pipes linking the Tactical Internet are even smaller. This proportionality will remain constant even as communication technology improves due to the mobility requirements demanded by the warfighter. The Tactical Internet is a highly mobile, common user, data network which provides data communications for the brigade down to the weapons platform level. Figure 18 represents the Tactical Internet which will also support the distributed information architecture of Athena.[14]

Large Information Nodes. Large Information Nodes (LINs) of the Athena network would be found at the MSE Node Centers to make maximum use of the large communication pipes between the nodes to supprt database updates and information queries. These nodes would contain the largest storage capacity and assume the responsibility to support user information requests and network manangement and maintenance. The LIN would consists of a two shelter configuration. The first shelter would consist of the heart of the system; a data storage capability, archieving capabilities, a large information processing capacity capable of multi-tasking, and communication interfaces with the local node center switch. The second shelter, the Information Management Center (IMC) would support network management and maintenance capabilities. Services provided would include, but not be limited to, information network monitoring and reconfiguration, troubleshooting, management of user access requests, and user support functions. Figure 19 depicts the LIN at an MSE node center.

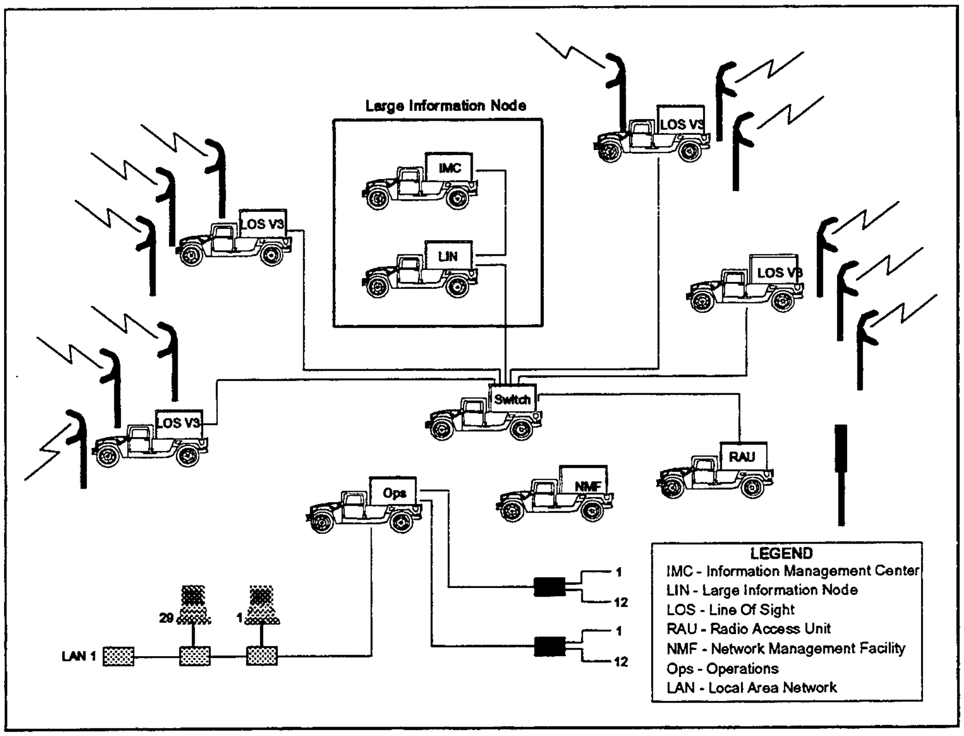

Figure 19. Large Information Node.

Medium Information Nodes. Medium Information Nodes (MINs) would be located at the subordinate MSE nodes (where LENs and SENs) are traditionally provided). MINs would support databasing and information processing requirements at the three division headquarters and the headquarters of the division's major subordinate commands. The MIN would also provide the interface with the entire division information pool thriugh the local digital switchboard and Line of Sight radio links to the LINs at the MSE node centers. MINs would be deployed in a single shelter configuration to support the mobility requirements of the supported headquarters. The IMC would be a remotable terminal to support network management and maintenance capabilities. Services provided would include, but not be limited to, information network monitoring and reconfiguration, troubleshooting, management of user access requests, and user support functions. Figure 20 depicts the MIN at an MSE LEN.

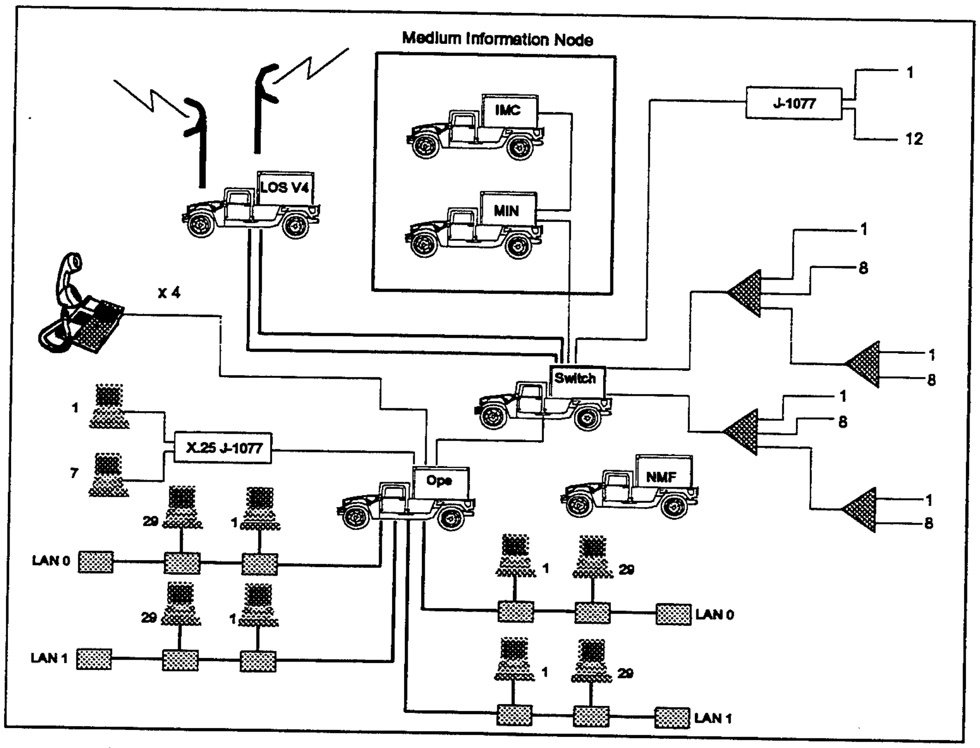

Figure 20. Medium Information Node at an MSE LEN.

Small Information Nodes. Small Information Nodes (SINs) would also be deployed at nodes of the Tactical Internet. The Tactical Internet is a common user data network to supprot information operations within the maneuver brigade. System Integration Vans (SIVs) within the maneuver brigade AO provide the communication nodes to support the Tactical Internet. SINs would be deployed at each SIV node that does not have access to MSE. SIN nodes would be smaller and support functions similar to those of the LIN and MIN. The system configuration would consist of one shelter that would provide the same capabilties as the MIN but at a reduced scale. The network operator position should be remotable to the SIV for optimal management of its portion of the network and provide the same management capability as the IMC. Figure 21 depicts the SIN at a Tactical Internet SIV site.[15]

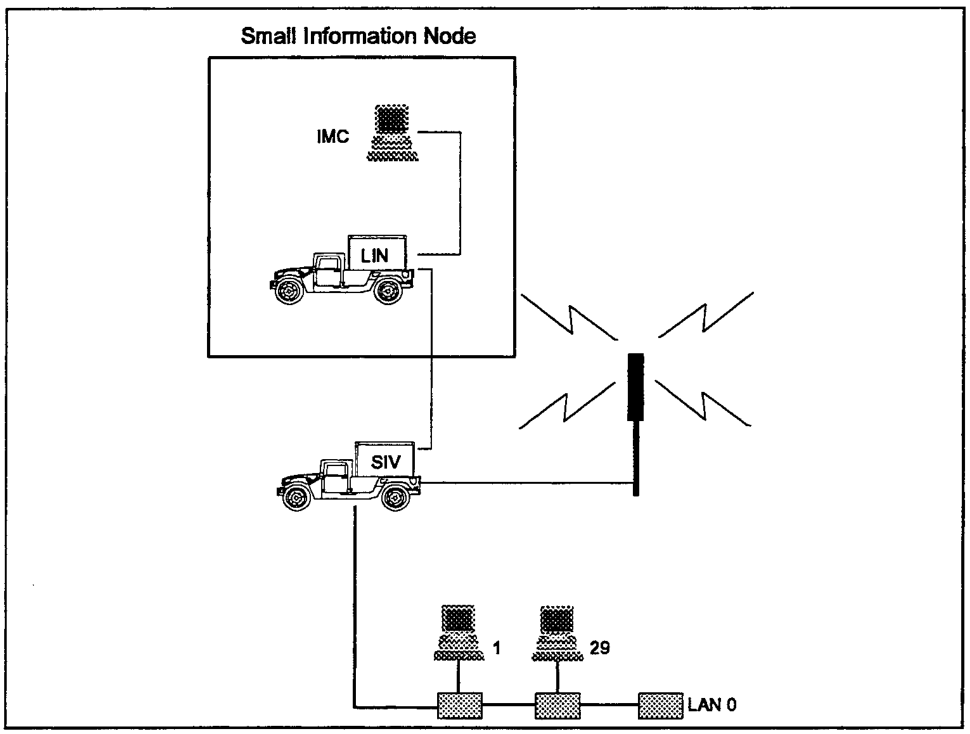

Figure 21. Small Information Node at a Tactical Internet SIV.

User Terminals. User terminals, as described above, should support rapid reconfigurationthat is transparent to the user. GUT terminals must be capable, through a communication server to select the most appropriate path to access any one of the LINs, MINs, or SINs. Regardless of the point of entry into the tactical information pool by the GUT the available information will appear to be coming from the same location, with access to the same amount of information.

It is also essential that the network maintain directory services to support user terminal intercommunication. On a fluid battlefield, users move throughout the communications network. During this movement, the Athena network must must maintain the ability to track any given user's location at any point in time. This must be accomplished automatically through the employment of a directory service that automatically registers user terminals across the network. The network as a whole must then be aware of each user's location to ensure timely transmission of data messages. This functionality should be transparent to the user.[16]

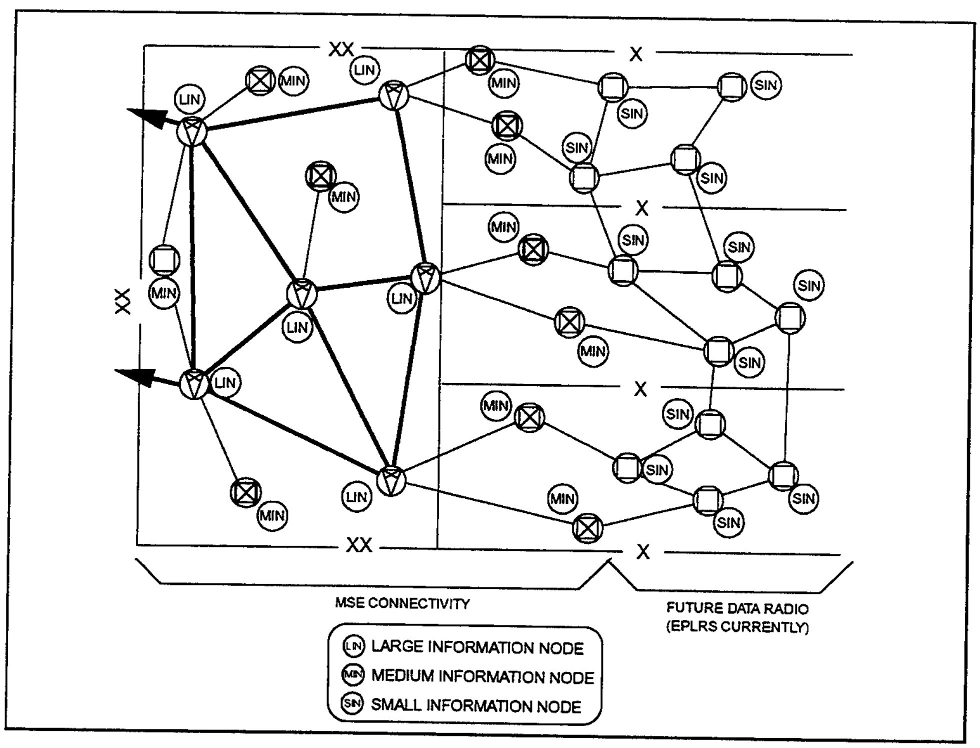

Figure 22. Athena's Battlefield Employment.

Athena Battlefield Laydown. The interconnection of the information nodes of the Athena architecture create a grid of connectivity among large capacity information machines. Together these nodes create the information pool which will support all user applications. The Athena network appears to each user as on large database of BOS immaterial information. This interconnectivity allows battlefield users to access a wide variety of information regardless of where is the information is stored. Figure 22 depicts the battlefield employment of the Athena Information Network.

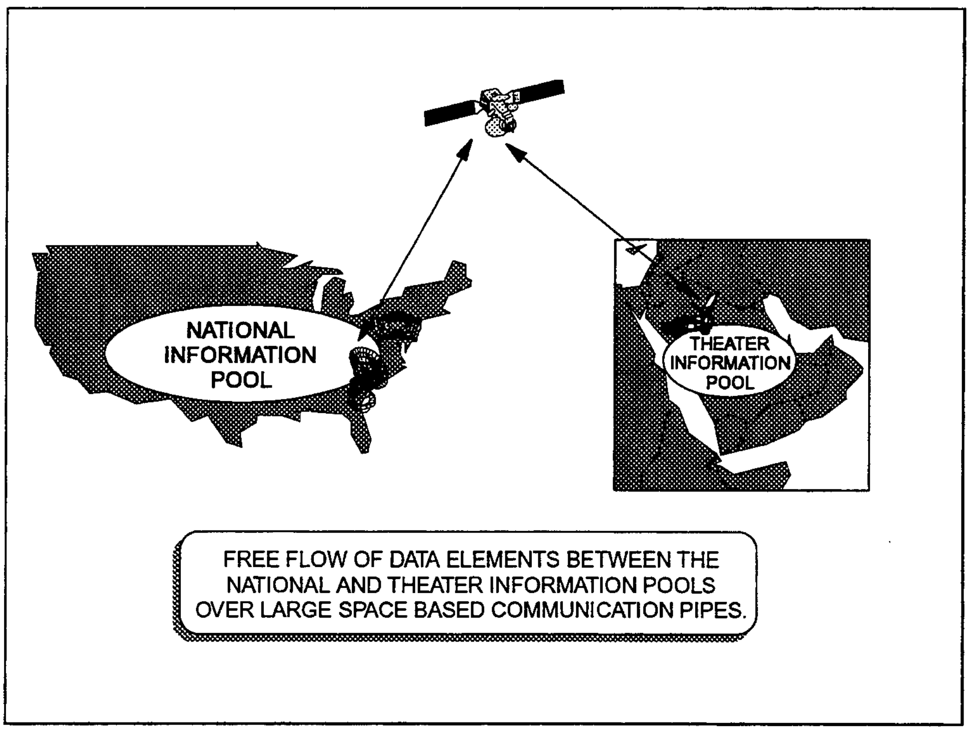

Figure 23. Connectivity with the National Information Pool.

Access to the national Information Pool. Once the tactical information pool is established, long haul communication pipes will be provided to support information exchange with the national information pool. This connectivity should be seamless and transparent to the user. Figure 23 represents the link between the tactical information pool and the national information pool.[17]

Since commercial technologies are moving towards a similar architecture, information access will include databases throughout the federal government; for example information on a particular enemy commander might be available in the Central Intelligence Agency's database. Warfighting commanders could access this information in near real-time and obtain a dossier on that commander and develop a course of action accordingly. This, of course, would depend upon the user's level of access. The bottom line is that information available within the national information pool would be as accesable to the warfighting commander as that information generated with the division AO.

Recommended Signal Structure in the Division. It is clear that the Athena architecture represents a redefinition of the Signal Corps. Signal support must therefore be redefined as communications and information support. The Signal Corps' experience in establishing and operating large communication networks as well as providing information services such as battlefiled LAN administration and E-Mail mark it as the prime candidate to assume proponency for information management on future battlefilelds.[18]

The Signal Corps must accept the challenge to become the Army's Information Corps. The Army will reap significant benefits from this action. Designating one branch for information proponency will ensure unity of effort in all future automation and communication endeavors.

It will eliminate the integration and interoperability problems found in stovepipe, legacy systems and help the Army move towards a single, contiguous information architecture. An Information Corps would also remove from the warfighting commander the burden of information management and focus his efforts on defeating the enemy.

Mission. The Signal Corps mission must be redefined to reflect the transistion from communications support to information support. Placing the entire information support mission under one branch ensures unity of effort in the management and development of information systems. It will create a focal point and direction for information technologies to meet the needs of the Army in the twenty-first century.

Current Signal Corps Mission.

> The mission of the Signal Corps is to provide rapid and reliable signal support for the command and control of the Army's combat forces during both peace and war. Signal Support is the collective, integrated, and synchronized use of information systems, services, and resources and it encompasses the following disciplines: automation, communications, visual information, records management, and printing and publication.
>
> 1. The ability to process and rapidly exchange information is one of the most criticakl elements in the effectiveness of today's modern military force. Every weapon system, command and control system, and service support system is becoming increasingly dependant on elctronics and automation, provided by the Signal Corps.
>
> 2. The Signal Corps encompasses Army units and elements engaged in the planning, design, engineering, acquisition, installation, operation, supply maintenance and evaluation of information systems at all levels within the Department of the Army and the Department of Defense.
>
> 3. In support of division, corps, and theater combined arms operations, the Signal Corps installs, operates and maintains a myriad of state-of-the-art, real-time, voice and data tactical information systems and provides battlefield information services.
>
> 4. At the strategic level, the Signal Corps engineers, installs, operates and maintains the Army's portion of the Defense

Information System (DIS) and its interface with tactical signal elements at theater and corps.

5. Together with its Air Force and Navy counterparts, the Signal Corps manages and directs the joint operation of the global corporate information management systems serving the Department of Defense and the National Command Authority.

6. In support of sustaining base operations, the Signal Corps engineers, installs, operates and maintains a variety of information services on all Army posts, camps, and stations.[19]

Restated Signal Corps Mission. The mission of the Signal Corps is to provide rapid and reliable signal support for the command and control of the Army's combat forces during both peace and war. Signal Support is the collective, integrated, and synchronized use and acquisition of information networks, services, and resources and it encompasses the following disciplines: automation, communications, visual information, records management, and printing and publication.

1. The ability to process and rapidly exchange information is one of the most critical elements in the effectiveness of today's modern military force. The Signal Corps provides the information networks and services to support effective comand and control.

2. The Signal Corps, for the Army, solely engages in the planning, design, engineering, acquisition, installation, operation, supply maintenance and evaluation of information systems at all levels within the Department of the Army and the Department of Defense. Additionally, as the sole combat developer for information networks, the Signal Corps ensures standardization and interoperability for all information and communication systems.

3. In support of division, corps, and theater combined arms operations, the Signal Corps installs, operates and maintains a

distributed information network encompassing state-of-the-art, real-time, voice and tactical information systems and provides battlefield information services.

4. At the strategic level, the Signal Corps engineers, installs, operates and maintains the Army's portion of the Defense Information System (DIS) and its interface with tactical signal elements at theater and corps for power projection operations.

5. Together with its Air Force and Navy counterparts, the Signal Corps manages and directs the joint operation of the global corporate information management systems serving the Department of Defense and the National Command Authority.

6. In support of sustaining base operations, the Signal Corps engineers, installs, operates and maintains a variety of information and communication networks and provides information services on all Army posts, camps, and stations.

Organization. The incorporation of information technology on the battlefield drives the need for an infrastructure. In order to achieve the full advantage to be gained by information technologies, signal units throughout the Army will have to be reorganized, to include the personnel and equipment, to support the information network.

Division Signal Battalion. Information node allocation must be aligned with the distribution of MSE nodes. The Division Signal Battalion of the heavy division consists of six node centers, one LEN, and twenty four SENs. An information node provided at each of these locations would require six LINs and twenty five MINs. A light division, with four node centers, on LEN and sixteen SENs would require four LINs and seventeen MINs. In a rapid deployment division a number of LENs and SENs have been replaced by Contingency Communication Packages (CCPs). The allocation of MINs applies equally to the CCPs in those divisions.

Signal Support in the Maneuver Brigade. The Tactical Internet is provided by fourteen SIVs, located at the maneuver brigade headquarters and the headquarters of the brigade's subordinate commands. However, only twelve SINs are required to support the brigade since two MINs are deployed to the brigade from the Division Signal Battalion. The MINs are deployed to the brigade headquarters and the Forward Support Battalion (FSB).

Personnel. The proposed information architecture implies an increase in manpower to support a network not previously provided. However, soldiers that currently support tactical record traffic systems could move to fill some of these positions. The additional manpower required would have to be found throughout the Army. New Military Occupation Specialties (MOSs) will also be required to support the installation, operation, and manintenance of the information systems that will collectively form the information network. Information Operation Specialists will be required to install, operate and maintain the information nodes located throughout the division AO. Each information node will also require Information Operation Ncos to manage the information facility and supervise assigned personnel. The S3 cell of the Signal Battalion will require two NCOs to perform as Information Network NCOs. These NCOs will be required to perform network level monitoring and troubleshooting of the Athena network. Previous experience as Information Operation NCOs will be critical to their performance of duties. Software analysts/programmers will be required at the Signal Battalion headquarters for on-the-fly software coding to support unique information requirements and to take corrective action when the network does not perform as needed. As technology continues to improve, the personnel requirements will be reduced accordingly. Table 1 depicts a recommended signal soldier allocation to support this architecture.[20]

	GRADE	HVY DIV SIG BN	LT DIV SIG BN	MNVR BDE (X3)	HVY DIV SUBTOTAL	LT DIV SUBTOTAL
LARGE INFORMATION NODE	E-6	6	4		6	4
INFO OPS NCO	E-5	6	4		6	4
INFO OPS SPEC	E-4	6	4		6	4
INFO OPS SPEC	E-4	6	4		6	4
INFO OPS SPEC	E-3	6	4		6	4
MEDIUM INFORMATION NODE						
INFO OPS NCO	E-5	25	17		25	17
INFO OPS SPEC	E-4	25	17		25	17
INFO OPS SPEC	E-3	25	17		25	17
SMALL INFORMATION NODE						
INFO OPS NCO	E-5			12	36	36
INFO OPS SPEC	E-4			12	36	36
SIG BN S3						
INFO NETWORK NCO	E-7	1	1		1	1
INFO OPS NCO	E-5	1	1		1	1
SOFTWARE ANALYST/PROGRAMMER	E-4	1	1		1	1
SOFTWARE ANALYST/PROGRAMMER	E-3	1	1		1	1
				TOTAL	**181**	**147**

Table 1. Information Architecture Manning Requirement.

Summary

The Information Architecture described herein represents a significant step forward in the use of information technologies to meet the demands of Army Operations. It frees the commander, his battlestaff, and his subordinate commanders from the burden of information management and focuses their efforts on mission accomplishment. It allows commanders to tailor their staff based on operational requirements, not battlefield functional areas. The architecture eliminates the need to assign personnel to update maps, copy overlays, and track down information. The information is available at the warfighter's fingertips. However, there is a price to be paid.

The price is an investment in the required infrastucture. Warfighting commanders must be willing to provide the personnel and the resources necessary to support the architecture for consolidation under the Signal Corps. The establishment of a single proponent for information management on the battlefield will act as a major combat multiplier. Current developmental efforts in information technologies are diffuse and lack significant impact. Consolidation of these efforts will gain synergy for the commander. Synergy on the battlefield allows the commander to mass the effects of the entire combat ubit at the decisive point at the optimal time within the battlespace. Information dominance is the key to victory on future battlefields for our Army. The described information architecture represents a clear path to the future, meeting today's warfighting requirements and those of the future.

---

[1]Grolier, "Athena", The New Grolier Multimedia Encyclopedia, (The Software Toolworks Inc, CA, 1993).

[2]MITRE Corporation, "Trends in Client/ServerTechnology," [http://peter.itsc.state.md.us/ITSC/techrepts/clntsrvr.html], 1996.

[3]Hayes, William, GTE Corporation, "Distributed Object Management," [http://info.gte.com/ftp/doc/notes/project-summary.html], 1996.

[4]Holsheiner, Marcel, CWI Corporation, "Data Mining: The Search for Knowledge in Databases," [http://www.cwi.nl/~marcel/papers.html], 1994.

[5]Directorate of Combat Developments, Modeling and Simulation ADO Study, (Fort Gordon, GA: United States Army Signal Center, 1996), p. 8.

[6]Loop, Tony, Warfighting Information Network and the Next Generation of Switches Using ATM Hub and ISDN White Paper, (Fort Gordon, GA: Directorate of Combat Developments, 1995), pp. 3-4.

[7]Center for Information System Security Defense Information Systems Security Program, Department of Defense Goal Security Architecture, Version 1.0, (Maryland: Government Printing Office, 1993), pp. 1-3.

[8]Headquarters, U.S. Army Training and Doctrine Command, Operational Requirements Document (ORD) for Army Battle Command Systems (ABCS), (Fort Monroe, VA: Govenment Printing Office, 1988), pp. 3-4.

[9]Biometric Journal, "Premier Issue of Biometric Journal Homepage," [http://www.icon-stl.net/~jsweeny/biometrics/bjournal.html], 1996, p. 1.

[10]Ibid., 2.

[11]Ibid., 3-4.

[12]Headquarters, Department of the Army, Common Operating Environment, (Washington, D.C.: Government Printing Office, 1995), p. 6.

[13]Headquarters, Department of the Army, Field Manual 11-43, The Signal Leader's Guide, (Washington, D.C.: Government Printing Office, 1995), pp. 3-1 - 3-4.

[14]Volz, Richard E., Jr., Tactical Internet for Task Force XXI White Paper, (Fort Gordon, GA: Directorate of Combat Developments, 1995), pp. 11-13.

[15]Ibid., 11.

[16]Headquarters, Department of the Army, Field Manual 24-7, Army Battlefield Command System (ABCS) System Management Techniques. (Washington, D.C.: Government Printing Office, 1995), pp. B8-B9.

[17]Headquarters, Department of the Army, U.S. Communications Electronics Command, Research, Development, and Engineering Center, Integrated Tactical to Strategic Data Network "Quick Fix" User Manual, Version 1, (Fort Monmouth, NJ: Executive Agent for Tactical Switched Syustems, 1994), pp. 1-3.

[18]Evans, Stanley E., "MOS 74B Information System Operator-Analyst," Army Communicator, Volume 20, Number 2, (Fort Gordon, GA: United States Army Signal Center, 1995), p. 42.

[19]Headquarters, Department of the Army, DA Pamphlet 600-3, Officer Personnel Update, (Washington, D.C.: Government Printing Office, 1993) pp. 4-1 - 4-2.

[20]Evans, Stanley E., "MOS 74B Information System Operator-Analyst," Army Communicator, Volume 20, Number 2, (Fort Gordon, GA: United States Army Signal Center, 1995), p. 41-43.

CHAPTER 5

CONCLUSIONS AND RECOMMENDATIONS

The Athena Information Architecture

The proposed Athena network represents an optimal solution that will meet the needs of warfighting commanders today and in the future. It is based upon the requirements of the warfighter and is developed as a single system, not a system of systems. User needs are met in the most efficient manner possible. The Athena network represents a culmination of the efforts of various Army combat developers, battle labs, program managers, research agencies, and a host of others. It presents a vision of information technologies on the battlefield of the twenty first century and a direction for future developmental efforts.

Commander's Critical Information Requirements (CCIR). The Athena network, as proposed herein, is driven by the needs of the commander. It's purpose is to place information in the hands of the commander that is critical to mission accomplishment. Athena does so in a manner that allows the commander to focus on the business of warfighting and alleviates the burden of information gathering and processing. However, commanders must recognize that information requirements do not consist of materiel solutions. Information requirements are those pieces of knowledge the commander must have in order to dissipate the fog of war and achieve information dominance.[1]

Network Organization. Any information network should be organized so that it attains the maximum benefit for the user. The Athena architecture is organized so that the complexity of the network is hidden from the user. This fundamental principle of network design reflects the implementations currently seen in modern communication networks as well as developing commercial information architectures.[2]

Commercial information service providers recognize that any information system which is difficult to use will be unacceptable to their customers. In order to remain competitive, information service providers are developing systems which facilitate their customer's ability to better manage information critical to their business' success.[3]

Transmission Efficiency. The Athena architecture achieves a balance between software transmission requirements and limited bandwidth. Communication resources on the battlefield with always be limited by the physics of the electromagnetic spectrum. It is therefore essential that battlefield information is transmitted in the most efficient method possible. The use of a distributed object-oriented database facilitates efficient movement of information over limited communication pipes.[4]

Provided Services. Any viable information network must take into account the services to be provided to the customer. The same is true of the Athena architecture. Athena is focused on providing the warfighter critical information, packaged in a usable format, in the smallest amount of time possible. Services should include user registration, formal messaging, security, user lookup, directory services, and routing. All of the requirements are encapsulated in the Athena Information Network.

Commercial R&D. In developing the Athena Information Network, it was essential to recognize the timelines required to field a system to the Army force structure. The long acquisition and fielding requirements, preclude the use of currently available commercial technologies. It was therefore necessary to investigate commercial research and development efforts in order to align possible Army implementation with the expected level of technology. It would not be prudent to design an optimal information architecture based on currently available technologies. Current technology would be obsolete by the time the Army fielded the network. Alignment with current commercial research and development efforts ensure the Army's ability to readily leverage commercial technologies well into the future.

Information Proponency. The described information architecture, Athena, demands a single proponent for all information management on the battlefield. This creates unity of effort in achieving information dominance. Single proponency ensures the development of a single contiguous information network, where the borders between information provided by the various BOSs become transparent to the user. This does not imply however that the information manager decides which information is available to the warfighter. The commander will remain the designator of CCIR.[5]

Signal Support. The best candidate for information proponency on the battlefield is the Signal Corps. The Signal Corps' expertise lies in employing and managing large communication networks.

Additionally, the signal brigades and battalions have assumed the responsibility to employ commercial information networks over tactical communication networks provide services such as electronic mail. This level of expertise across all the BOSs uniquely qualifies the Signal Corps to assume the role of battlefield information manager. It then is a matter of redefining signal support. Signal support should now be defined as providing both information and communication networks across the battlefield.[6]

Infrastructure Investment. The employment of information systems across the battlefield represents a new capability for the warfighting commander. However, the capability provided by the Athena architecture has a price in manpower and materiel. Approximately one company of signal soldiers will be required as well as the information nodes themselves. This cost is relatively minimal when compared against the cost of developing, fielding, and training the myriad of systems currently under development. the Athena architecture requires an investment in the Army's infrastructure; a face lift that will be needed if America's Army is to achieve information dominance on the battlefields of the twenty-first century.

Benefits to the Warfighter

The Athena Information Network represents a quantum leap forward in the capabilities provided to the warfighter. It provides the means to produce the synergy of information on the battlefield.

Synergy. Synergy is achieved through the integration between echelons within a single BOS and through synchronization among all the

BOSs. A distributed, object-oriented information network, such as Athena, enables the attainment of this goal. Synergy can only be achieved through the unimpeded flow of information among the BOSs and all Army echelons. Athena represents the means necessary to ensure the seamless flow and correlation of battlefield information that win enable Army commanders to win on the battlefields of the future. Athena is a single system, not a system of systems that require unique interfaces that achieve minimal interoperability.[7]

Cost. Cost is one of the most significant factors in the development of any information network. As the Army's budget continues to shrink, it is imperative that redundant developmental efforts be eliminated. The Athena Information Network makes this possible. As a single system, Athena will eliminate all redundant systems capabilities that are currently funded under the various information system programs.

The Athena architecture is based upon emerging commercial trends; that of a two tiered structure consisting of the user and the network. The user end of developing commercial architectures consists of a variety of low-end terminal devices that gain their information handling power from the network into which they are connected. The overarching information network consists of a series of interconnected databases which share information in a seamless manner. These information networks employ object-oriented databases to facilitate the correlation of information and the generation of information products.[8]

User Burden. The GUT terminals of the Athena architecture provide a single family of low-end user terminals that can be employed at any echelon. These terminals should be simple to operate. This principle allows warfighting commanders to focus on developing unique solutions to unique problems on the battlefield. GUT terminals should be capable of rapid configuration to support the individual user's information requirements. Additionally, all network services that are provided should require minimal interface by the user, such as security and user registration.[9]

Survivability. Athena gains its survivability from its distributed architecture. The network layer of the architecture is created by interconnecting a series of information nodes. These information nodes are dispersed throughout the division area of operations and replicate stored information at adjacent information nodes. Replicating the databases ensures survivability of the information contained therein. Loss of an information node does not constitute the loss of information.

Further Investigation

This thesis has attempted to investigate the information needs of warfighting commanders and their staffs. It has proposed an optimal information structure best suited to meet those needs. The Athena architecture is a system level proposal for an information structure within a division of the twenty-first century. The Athena proposal should be viewed as a vision of where the Army should be going; a goal for the future. Determining the means for its implementation is an Army wide task. Further investigation, therefore, is warranted in a number of areas.

Migration of the Current C4I Architecture. The first effort that should be made if Athena is to become the Army's objective information architecture is an examination of current information systems. Each system structure should be examined in detail to determine its potential for migration into a distributed computing environment. A close inter-relationship with commercial industry will be essential if current systems are to be brought into the Athena structure.

Corps to the Sustaining Base. The Athena architecture, for the purpose of this thesis, has been limited in scope to division level and below. However, the basic fundamentals of the network structure can be applied from the foxhole to the sustaining base. A serious investigation should be made into the ramifications of this architecture on the Army's fixed infrastructure and Army echelons above the division level.[10]

Joint Information Networks. The trend is clear that all military operations in the future will be joint in nature. The proposed Athena Information Network should also be considered as the information solution for the joint community. A single seamless information system would create synergy for joint operations. The interoperability challenges experienced today would be to a large part eliminated. A parallel effort at the Department of Defense (DoD) and the joint warfighting level should be instituted.[11]

Battle Lab Efforts. Every Army Battle Lab is involved in the development of command and control systems. Most materiel solutions assume unlimited communication support which is simply not the case.

Information requirements will always grow faster than the communication pipes will be able to support. Athena establishes a blueprint into which each Battle Lab command and control product must fit. Two such examples of this are the Mobile Strike Force and the numerous Advanced Warfighting Experiments.

Mobile Strike Force (MSF). The MSF is a study currently conducted at Fort Leavenworth to determine the organization, tactics, techniques, and procedures for an Army division in the year 2010. The fundamental premise of MSF is the attainment of information dominance on the battlefield at the decisive point. Information dominance can be readily achieved through the employment of Athena. It is highly recommended that the Athena architecture be evaluated as the system to support the MSF.[12]

Advanced Warfighting Experiments. Current efforts tend to be diffuse and lack a sufficient exploration of the impact of a proposed system on the network as a whole. Athena represents a goal for all Army information and communication systems. As such, it will create unity of effort for all AWEs that focus on automated command and control. AWEs can then focus on finding commercially available solutions that will help bring the total architecture to fruition.

Summary

This thesis has attempted to propose an objective information architecture for the Army of the twenty-first century: Athena. Athena represents the union of warfighting requirements and emerging information and communication technologies. Athena is a blueprint for the future of Army, and possibly joint, command and control. It is critical that the Army adopt a single vision for battlefield information systems if it is to achieve information dominance over America's potential enemies.

---

[1] Headquarters, Department of the Army, Field Manual 34-1, Intelligence and Electronic Warfare Operations, (Washington, D.C.: Government Printing Office, 1994), p. 2-17.

[2] Holsheimer, Marcel, CWI Corporation, "Architectural Support for Data Mining," [http://www.cwi.nl/~marcel/papers.html], 1994.

[3] Zysman, George I., "Wireless Networks," Scientific American, (New York, New York: Scientific American, Inc., September, 1995), pp. 70-71.

[4] Advanced database Systems Laboratory, "Object-Oriented Database Systems," [http://www.cs.umanitoba.ca/%7Edbgroup/distributed_DBS.html], 1996.

[5] Headquarters, Department of the Army, Field Manual 34-1, Intelligence and Electronic Warfare Operations, (Washington, D.C.: Government Printing Office, 1994), p. 2-17.

[6] Buchholz, Douglas D., Chief Signal Officer Notes, (Fort Gordon, GA: United States Army Signal Center, 1995), p. 6.

[7] Herbert, Paul H., Deciding What has to be Done: General William E. DePuy and the 1976 Edition of FM 100-5, Operations, (Washington, D.C.: Government Printing Office, 1988), pp. 6-9.

[8] Zysman, George I., "Wireless Networks," Scientific American, (New York, New York: Scientific American, Inc., September, 1995), pp. 69-71.

[9] Headquarters, U.S. Army Training and Doctrine Command, Operational Requirements Document (ORD) for Army Battle Command Systems(ABCS), (Fort Monroe, VA: Government Printing Office, 1993), pp. 12-13.

[10] U.S. Army Training and Doctrine Command, Force Projection Army C4I Support, (Fort Monroe, VA: Government Printing Office, 1993), p. 3.

[11] Defense Information Systems Agency Joint Interoperability and Engineering Organization, Joint Task Force Tactical Communications Architecture, (Washington, D.C.: Governemnt Printing Office, 1995), pp. 2-1 - 2-5.

[12] Headquarters, Department of the Army, Field Manual 71-100, (Draft), (Washington, D.C.: Governemnt Printing Office, 1995), pp. 1-8.

BIBLIOGGRAPHY

Books

Bateman, Robert S. Asynchronous Transfer Mode (ATM) Technology and Applications Version 3.0. Georgia: AT&T Bell Laboratories, 1995.

Beam, Walter R. Command, Control, and Communications Systems Engineering. New York: McGraw-Hill Publishing Company, 1989.

Campen, Alan D. The First Information War. Virginia: AFCEA International Press, October 1992.

Periodicals and Articles

Cooper, Pat. "DOD Official Pushes Civilian Technology Lift." Defense News 11, No. 6 (1996): 16.

________. "U.S. Army Examines Initial Battlefield Imagery Data." Defense News, 10, No. 45 (1995): 22.

Evans, Stanley E. "MOS 74B Information System Operator-Analyst." Army Communicator, 20, No. 2 (1995): 41.

Lenat, Douglas B. "Artificial Intelligence." Scientific American. New York, New York: Scientific American, Inc., September 1995.

Maes, Pattie. "Intelligent Software." Scientific American. New York, New York: Scientific American, Inc., September 1995.

Zysman, George I. "Wireless Networks." Scientific American. New York, New York: Scientific American, Inc., September 1995.

Government Documents

Army Science Board. Army Science Board Summer Study. Washington, D.C.: Government Printing Office, 23 September 1994.

Assistant Secretary of Defense for Command, Control, Communications and Intelligence. Memorandum for Director, National Security Agency.

Use of FORTEZZA to Protect Classified Information. Washington, D.C.: Government Printing Office, 1995.

Buchholz, Douglas D., MG. Chief of Signal Notes. Fort Gordon, GA: United States Army Signal Center, 1995.

Center for Information System Security Defense Information Systems Security Program. Department of Defense Goal Security Architecture, Version 1.0. Maryland: Governemnt Printing Office, 1993.

Chairman, Joint Chiefs of Staff. C4I for the Warrior. Washington, D.C.: Government Printing Office, 1993.

Defense Communications Agency, Joint Tactical Command, Control, and Communication Agency. Functional C3 Interoperability Architecture for Land Combat Operations. Washington, D.C.: Government Printing Office, 1995.

Defense Information Systems Agency, Joint Interoperability and Engineering Organization. Joint Task Force Tactical Communications Architecture. Washington, D.C.: Government Printing Office, 1995.

Defense Information Systems Agency. Allied Communications Publication 123 Tactical Requirements Analysis. McLean, VA: Government Printing Office, 1993.

Department of the Army, Headquarters, U.S. Army Communications Electronics Command, Research, Development, and Engineering Center. Integrated Tactical to Strategic Data Network "Quick Fix" User Manual, Version 1. Fort Monmouth, NJ: Executive Agent for Tactical Switched Systems, 1994.

Department of the Army. 93d Signal Brigade After Action Report for Operations Desert Shield and Desert Storm. Germany: 93d Signal Brigade, 1992.

________. C4I Technical Architecture. Washington, D.C.: Government Printing Office, 1995.

Director of Combat Developments. Army Common User System System Improvement Plan. Fort Gordon, GA: Signal Center, 1993.

Director of Information Systems for Command, Control, Communications, and Computers. Army Enterprise Strategy...The Vision. Washington, D.C.: Government Printing Office, 1993.

________. Army Enterprise Strategy. Washington, D.C.: Government Printing Office, 1994.

________. Department of the Army C4I Technical Architecture, Version 2.5. Washington, D.C.: Government Printing Office, 1993.

Directorate of Combat Developments. Modeling and Simulation ADO Study. Fort Gordon, GA: United States Army Signal Center, 1996.

________. Regimental Officer's Academy. Fort Gordon, GA: United States Army Signal Center, 1995.

Headquarters, Department of the Army. Field Manual 24-7, Army Battle Command System (ABCS) System Management Techniques. Washington, D.C.: Government Printing Office, June 1995.

________. Field Manual 100-5, Army Operations. Washington, D.C.: Government Printing Office, 1993.

________. Field Manual 24-17, Tactical Record Traffic System. Washington, D.C.: Government Printing Office, 1991.

________. Field Manual 11-43, The Signal Leader's Guide. Washington, D.C.: Government Printing Office, June 1995.

Headquarters, U.S. Army Communications Electrionic Command. Command, Control, Communications, Computers, Intelligence, and Electronic Warfare (C4IEW) Project Book. New Jersey: Fort Monmouth, 1995.

Headquarters, U.S. Army Training and Doctrine Command. Operational Requirements Document (ORD) for Army Battle Command Systems (ABCS). Fort Monroe, VA: Government Printing Office, 1993.

Joint Interoperability Engineering Office (JIEO). JTF Tactical Communications Architecture. Washington, D.C.: Government Printing Office, January 1995.

Loop, Tony. Warfighter Information Network and the Next Generation of Switches Using ATM Hub and ISDN White Paper. Fort Gordon, GA: Directorate of Combat Developments, 1995.

Loral Federal Systems. Defense Message System. Virginia: Loral Federal Systems, 1995.

Office of the Secretary of Defense (OSD). Functional C3 Interoperability Architecture for Land Combat Operations. Washington, D.C.: Government Printing Office, 28 January 1991.

Thompson, Henry L. "The High Performing Staff." Army Organizational Effectiveness Journal. Washington, D.C.: Government Printing Office, 1984.

Training and Doctrine Command. Force Projection Army C4I Support. Virginia: Government Printing Office, 1993.

U.S. Army Information Systems Command. Defense Message System Army (DMS Army) Tactical Architecture and Transition Strategy (Draft). Fort Huachuca, AZ: Government Printing Office, 1994.

U.S. Army Signal Center. Force XXI, The Signal Training Vision. Fort Gordon, GA: United States Army Signal Center, 1995.

U.S. Army Signal Center. Siganl Corps Pamphlet. Fort Gordon, GA: United States Army Signal Center, 1994.

U.S. Army Signal Center. The Army Satellite Communications (SATCOM) Architecture. Fort Gordon, GA: TRADOC System Manager, 1996.

Volz, Richard E. Tactical Internet for Force XXI White Paper. Fort Gordon, GA: Directorate of Combat Developments, 1995.

World Wide Web

Advanced Database Systems Laboratory. "Distributed Database Systems." [http://www.cs.umanitoba.ca/%7Edbgroup/distributed_DBS.html]. 1996.

Advanced Database Systems Laboratory. "Object-Oriented Database Systems." [http://www.cs.umanitoba.ca/%7Edbgroup/distributed_DBS.html]. 1996.

Biometric Journal. "Premier Issue of Biometric Journal Homepage." [http://www.icon-stl.net/~jsweeny/biometrics/bjournal.html]. 1996.

Hayes, William. "Distributed Object Management." [http://info.gte.com/ftp/doc/notes/project-summary.html]. 1996.

Holsheimer, Marcel. "Data Mining: The Search for Knowledge in Databases." CWI Corp. [http://www.cwi.nl/-marcel/papers.html]. 1994.

Holsheimer, Marcel. "Architectural Support for Data Mining." CWI Corp. [http://www.cwi.nl/-marcel/papers.html]. 1994.

Lee, Min. "Parallel and Distributed Computing Research Laborartory." [http://eagle.cs.cuhk.hk/]. August, 1995.

MITRE Corporation. "Trends in Client/Server Technology." [http://peter.itsc.state.md.us/ITSC/techrpts/clntsrvr.html]. 1996.

INITIAL DISTRIBUTION LIST

1. Combined Arms Research Library
U.S. Army Command and General Staff College
1 Reynolds Ave.
Fort Leavenworth, KS 66027-1352

2. Defense Technical Information Center
Cameron Station
Alexandria, VA 22314

3. Commander
USASC&FG
ATTN: MG Douglas D. Buchholz
Fort Gordon, GA 30905

4. Defense Information Systems Agency
Vice Director's Office
701 S. Courthouse Road
Arlington, VA 22204-2199

5. Commander
USASC&FG
ATTN: COL Robert L. Forrester
Fort Gordon, GA 30905

6. Major Howard Couzzi
CTAC-PW
USACGSC
1 Reynolds Ave.
Fort Leavenworth, KS 66027-1352

7. Major Deborah Valentine
TPIO-ABCS
Combined Arms Command
Fort Leavenworth, KS 66027-1352

8. SFC John T.Broom
CSI
USACGSC
1 Reynolds Ave.
Fort Leavenworth, KS 66027-1352

CERTIFICATION FOR MMAS DISTRIBUTION STATEMENT

1. Certification Date: 5 / 12 / 96

2. Thesis Author: MAJOR Richard E. Volz, Jr.

3. Thesis Title: An Objective Information Arcitecture for the Army of the Twenty-First Century: Courting Athena

4. Thesis Committee Members Signatures: Howard Crosby

5. Distribution Statement: See distribution statements A-X on reverse, then circle appropriate distribution statement letter code below:

A B C D E F X SEE EXPLANATION OF CODES ON REVERSE

If your thesis does not fit into any of the above categories or is classified, you must coordinate with the classified section at CARL.

6. Justification: Justification is required for any distribution other than described in Distribution Statement A. All or part of a thesis may justify distribution limitation. See limitation justification statements 1-10 on reverse, then list, below, the statement(s) that applies (apply) to your thesis and corresponding chapters/sections and pages. Follow sample format shown below:

S-----------SAMPLE---------SAMPLE---------SAMPLE----------SAMPLE-------S

Limitation Justification Statement	Chapter/Section	Page(s)
Direct Military Support (10)	Chapter 3	12
Critical Technology (3)	Sect. 4	31
Administrative Operational Use (7)	Chapter 2	13-32

----------SAMPLE---------SAMPLE----------SAMPLE----------SAMPLE-------

Fill in limitation justification for your thesis below:

Limitation Justification Statement	Chapter/Section	Page(s)

7. MMAS Thesis Author's Signature: ____________________

STATEMENT A: Approved for public release; distribution is unlimited. (Documents with this statement may be made available or sold to the general public and foreign nationals.)

STATEMENT B: Distribution authorized to U.S. Government agencies only (insert reason and date ON REVERSE OF THIS FORM). Currently used reasons for imposing this statement include the following:

1. Foreign Government Information. Protection of foreign information.

2. Proprietary Information. Protection of proprietary information not owned by the U.S. Government.

3. Critical Technology. Protection and control of critical technology including technical data with potential military application.

4. Test and Evaluation. Protection of test and evaluation of commercial production or military hardware.

5. Contractor Performance Evaluation. Protection of information involving contractor performance evaluation.

6. Premature Dissemination. Protection of information involving systems or hardware from premature dissemination.

7. Administrative/Operational Use. Protection of information restricted to official use or for administrative or operational purposes.

8. Software Documentation. Protection of software documentation--release only in accordance with the provisions of DoD Instruction 7930.2.

9. Specific Authority. Protection of information required by a specific authority.

10. Direct Military Support. To protect export-controlled technical data of such military significance that release for purposes other than direct support of DoD-approved activities may jeopardize a U.S. military advantage.

STATEMENT C: Distribution authorized to U.S. Government agencies and their contractors: (REASON AND DATE). Currently most used reasons are 1, 3, 7, 8, and 9 above.

STATEMENT D: Distribution authorized to DoD and U.S. DoD contractors only: (REASON AND DATE). Currently most used reasons are 1, 3, 7, 8, and 9 above.

STATEMENT E: Distribution authorized to DoD only; (REASON AND DATE). Currently most used reasons are 1, 2, 3, 4, 5, 6, 7, 8, 9, and 10.

STATEMENT F: Further dissemination only as directed by (controlling DoD office and date), or higher DoD authority. Used when the DoD originator determines that information is subject to special dissemination limitation specified by paragraph 4-505, DoD 5200.1-R.

STATEMENT X: Distribution authorized to U.S. Government agencies and private individuals of enterprises eligible to obtain export-controlled technical data in accordance with DoD Directive 5230.25; (date). Controlling DoD office is (insert).